Attachment A

SECURUS Detailed Technical Response

(3) TECHNICAL PROPOSAL

Understanding of Work and Plan for Service

Describe in detail your understanding of the work that is to be performed as presented in Sections Four and Five of this RFP. Offerors must provide a comprehensive narrative statement that illustrates their understanding of the requirements of the services and outcomes to be achieved.

Additionally, offerors must provide a comprehensive narrative statement that sets out their plan for providing the services and illustrates how their plan will serve to accomplish the work addressed in Section Five of this RFP. This section of the proposal must include a proposed work schedule for providing the services, to include all items specified in Section 5 of this RFP.

This section should not merely paraphrase the scope of services from the RFP. This section must demonstrate an understanding of what has been requested, the major issues involved, and what must be done to accomplish the objectives.

Include in this section how much travel is anticipated in the performance of this contract.

If you are providing a proposal that utilizes a subcontractor approach with one or more firms, you must detail how each firm's work will assist in the work to be performed.

Understanding of Work

SECURUS Technologies, Inc. through its wholly owned subsidiary, Evercom Systems, Inc., proposes to pay a commission to the Alaska DOC and to provide a state-of-the-art Inmate Telephone System (ITS). Our services include a turnkey system and all related services including hardware and software; installation, maintenance, optimization and training; connectivity, data storage and support; call origination and connection to the billed party number including call rating and billing; and a comprehensive suite of client applications and features including call blocking, call duration limits, centralized call monitoring and recording, investigative and security controls, PINs and 3-Way Call Detection and Collect and Prepaid Calling Capabilities.

Plan for Services

As Alaska DOC's Inmate Telephone Service provider for the past 10 years we offer a thorough understanding of the unique needs and challenges faced by the Alaska DOC. Our Alaska based field technician, Jasen Kitner understands and delivers site specific support to insure maximum system reliability given the challenges of site locations and weather including site visits throughout the year for maintenance, training and investigative support. A description of the steps involved in an implementation is included below, and a detailed project plan is available in *Attachment H – SECURUS Preliminary Project Plan*.

Project Controls and Quality Checks

Timely execution and completion will be monitored by using scheduled completion dates in correcting implementation or operational problems, as well

as problems reported through SECURUS' trouble reporting system. Summary reporting, trend analysis, and schedule monitoring facilitates tracking problem correction.

Other less formal reviews of installation status are held throughout the installation process. Operations staff meetings provide the Implementation Manager. Installation Manager and Lead Project Manager with periodic status, and allow coordination and dissemination of the information to SECURUS Installation field technicians.

Transition Period with Minimum Service Disruptions
Because SECURUS is the current provider, transition downtime will be minimal, if any. By installing all SECURUS equipment and circuits prior to the cutover date, usually one to two weeks in advance of the cutover date, this allows for all systems, circuits, etc., to be fully tested. By fully testing prior to cutover, there will be no risk of service interruptions due to the changeover to the new SECURUS ITS system. The SECURUS team has used this process with much success throughout our multiple accounts in the US and Canada.

SECURUS will have installed and tested all necessary equipment and circuits prior to the actual cutover date. There will not be any interruption of service. The cutover may be conducted during the time the facility has all phones off, i.e., a count time, prior to the phones coming on at the beginning of the day or after the phones go off for the day. This will minimize any downtime for the facility.

Software Programming and Preparation
After meeting with personnel from the Alaska DOC, internal meetings will be held between Project Management and Install team to review the validation process that will be used to ensure that the system conforms to the functional facility requirements.

Prior to shipment systems are fully tested and to ensure that the ITS system can be successfully implemented at the Alaska DOC sites. Hardware design will be performed for each site to be installed. After the site surveys are confirmed all site requirements will be identified and a Bill of Lading (BOL) will be prepared. The Bill of Lading will be provided to the Alaska DOC to ensure all parties agree to the items and their quantities. The system equipment is assembled and forwarded to a staging and testing area prior to shipment. The system is typically shipped two weeks prior to cutover.

In order to replicate of inmate profile information located in the existing Personal Identification Numbers (PIN) and Personal Allowed Numbers (PAN) database, SECURUS will transfer this data from our existing inmate call platform. SECURUS will work closely with Alaska DOC to ensure accurate and timely information is imported immediately prior to final cutover at each institution. The process will require data entry of new residents at each facility to be held while file conversion, testing of data integrity and deployment takes

place. Once the new database and telephone service are restored, new resident profile information will be entered directly into the new SECURUS system.

Testing
A series of testing procedures are conducted by the field technician as itemized:

- **Place local Calls and listen to voice prompts**
- **Select Spanish prompts**
- **Place intraLATA, and interLATA calls**
- **Attempt to call blocked numbers**
- **Print sample call detail reports at the workstation**
- **Verify that site received user manuals**
- **Confirm and Test Prepaid calling**
- **Attempt a 3-Way call**
- **Listen/monitor and active call**
- **Query Recorded Call information**
- **Place a call to a privileged number**
- **All recording and monitoring functions**
- **Assign and test PIN accounts. Complete Test calls for PINs**

The major tasks involved in a standard ITS installation are detailed below.

Task Name
Contract Signed
Implementation Meeting Held with designated Alaska DOC personnel and SECURUS Project Team Personnel • **Establish site contact personnel from the DOC** • Establish ITS rollout schedule and approval by Alaska DOC • Finalize feature set selection • Verify Findings from Site Surveys of All Locations • Identify special need phones, i.e. TTY/TDD, portable/moveable phones • Review Alaska DOC policy and procedures/ security clearances for SECURUS installation teams
SECURUS Project Team Meetings
Conversion Plan Evaluated & Adjusted as Necessary During Weekly Internal Conference Calls Through-out Project Duration • Confirm install dates with Master Scheduler • Review Final Plan with Installation Teams • Confirm Install Support • Confirm Shipping • Confirm Training
Order/Install Lines for all locations • T1's/Analog Lines/Frames
Feature Selection Confirmed
Obtain Line Numbers and Confirm Orders and Due Dates with Local Exchange Company
Branding Messages Developed
Configure ITS

Task Name
Quality Control ITS test • Feature testing • System testing • Load testing * All quality control is conducted in Dallas prior to ship.
Package & Ship Equipment to Delivery Location
Installation of ITS • Receive and inventory equipment • Build equipment • Prepare to cut ITS – Power-up ITS – Install workstations – Conduct install test – Coordination with Install Support – Install blocked number table, free numbers, and inmate PINs/PANs • Replace inmate telephone sets
Cutover of ITS • Notify facility that cutover will occur and gain Site/Central office approval to proceed • Cutover system at agreed upon time to minimize disruption • Notify facility of cut
Quality Assurance of ITS and Acceptance Testing Complete
Training of Facility Personnel

Continued Support

SECURUS maintains a centralized 24/7/365 Network Operations Center (NOC) and technical support center in the greater Dallas, TX, area to monitor operations and ensure maximum operational status. In addition, a dedicated Field Service Technician will be based in Alaska to provide service response to any site for hardware or software issue. A service escalation contact list will be provided to each site.

In addition as the current ICS provider our field technician has historically completed the following annual field support activity and we believe this is part of our ongoing commitment to service the Alaska DOC.

	Preventive Maintenance	Handset Repairs	Misc Phone Issues	Installation - Additions and Moves	System and Network Issues
AK - ANCHORAGE JAIL	5	50	10	1	2
AK - ANVIL MT.	1	5	8		
AK - COOK INLET	3	33	17	1	5
AK - FAIRBANKS	1	26	17	1	3
AK - HILAND/MEADOW	3	12	10		5
AK - KETCHIKAN	1	12	7	1	1
AK - MATSU	3	8	13	1	
AK - PALMER	3	16	14	2	10
AK - POINT MACKENZIE	1		11	1	2
AK - SPRING CREEK	1	10	21	1	1
AK - WILDWOOD	4	23	14		1

	Preventive Maintenance	Handset Repairs	Misc Phone Issues	Installation - Additions and Moves	System and Network Issues
AK - YUKON-KUSKOKWIM	1	19	7		
AK - LEMON CREEK	1	30	10		1
Totals	28	244	159	9	31

5.01
Scope of Work

The State of Alaska intends to contract for services to provide current state of the art inmate telephone system and necessary billing services in each of it's correctional facilities. The correctional institutions are located in Anchorage, Nome, Fairbanks, Eagle River, Ketchikan, Juneau, Palmer, Wasilla, Seward, Kenai, and Bethel, Alaska. The State also reserves the right to add additional facilities during the life of the contract.

☑ **SECURUS has read and understands.**

The Contractor will provide all inmate telephone systems and monitoring equipment, installation, optimization, training, and ongoing operation of the systems. All costs of equipment, installation, optimization, training and ongoing operation of the systems are the responsibility of the Contractor. All equipment installed by the Contractor at the correctional facilities will remain the sole and exclusive property of the Contractor. The State will not be responsible for any damage to equipment including damage caused by inmates. **The system must be a "turn-key" system. The successful contractor will be required to install a new Inmate Telephone System that is "state of the art" technology.**

☑ **SECURUS has read and will comply.**

SECURUS' role as a "Single Source / Single Point" provider ensures the Alaska DOC will make only one call to receive world class service and support 24/7/365. The Alaska DOC will benefit greatly from dealing directly with the architect of the Secure Call Platform (SCP), SECURUS, without going through an unnecessary "Middle Man" While most vendors resell and lease another company's platform, we designed our own, which means the Alaska DOC will have a direct influence on future upgrades and functionality. SECURUS is committed to providing technically advanced solutions for the future in an effort to ensure the Alaska DOC has the technology and tools to fight crime, decrease costs, and increase revenues.

Inmate telephone system equipment identified by brand name within this document is for comparison purposes only. Actual telephone system equipment used or provided by the contractor must meet or exceed the specified equipment capabilities and capacities as set forth in the specifications. All equipment and materials furnished under the contract resulting from this RFP must be the latest "state of the art" technology. The State reserves the right to

approve minor deviations from the specifications if it is determined to be in its best interest.

☑ **SECURUS has read and will comply.**

5.02
System Requirements

Tables One, Two, Three and Four provide the following information. This information should not be construed as a guarantee of call activity or the number of phones to be installed in any one institution.

1. Number of inmates per institution. (Table One)
2. Number of inmate phones presently used at each institution. (Table One)
3. Telephone utilities serving the various institutions. (Table Two)
4. Number of intrastate calls made by institution during a 12 month period with total number of minutes involved. (Table Three)
5. Number of interstate calls made by institution during a 12 month period with total number of minutes involved. (Table Four)
6. Call Revenues (Table Five)

☑ **SECURUS has read and will comply.**

The contractor shall be responsible for obtaining all required approvals from the Regulatory Commission of Alaska (RCA) for performance under the resulting contract within 60 days of contract award.

☑ **SECURUS has read and will comply with the understanding that upon contract award, tariffs for local collect calling will be filed immediately with the Regulatory Commission of Alaska. Delays beyond the control of SECURUS do to RCA's untimely approval of applicable tariff's should not be considered as a failure to perform.**

The successful contractor shall reimburse the Department of Corrections for the cost of state personnel time, travel, and per diem involved in quality assurance and acceptance testing of the systems. For budgetary purposes, the State of Alaska has determined a budgetary figure of $50,000.00 for this cost. The successful Offeror shall reimburse the Department of Corrections for these costs upon final acceptance of the entire system.

☑ **SECURUS has read and will comply.**

The successful contractor will pay the State of Alaska, Department of Corrections (DOC) a guaranteed yearly dollar payment over the life of the contract. This payment shall be made in quarterly payments over each year on a schedule subject to approval of the Contractor and DOC. Payments must be made based upon gross revenues received from connection fees and per minute charges. **Local calls from pre-trial booking phones must be free. Charges will apply to all other local calls.**

☑ **SECURUS has read this requirement and responded in the Cost Proposal as required.**

A late payment is subject to 1.5% interest per month on the unpaid balance.

☑ **SECURUS has read and understands.**

Offerers must provide a pre-qualifying statement showing that they have experience in providing an inmate phone system similar to the system required by this RFP. Offerers must provide a list of at least 4 systems (including phones and monitoring systems) comparable in size and complexity to the system currently in use by DOC that have been successfully installed and operated by the offeror. The list must include contact names, addresses and phone numbers. **Failure to provide the information described in this paragraph will result in your proposal being found non-responsive.**

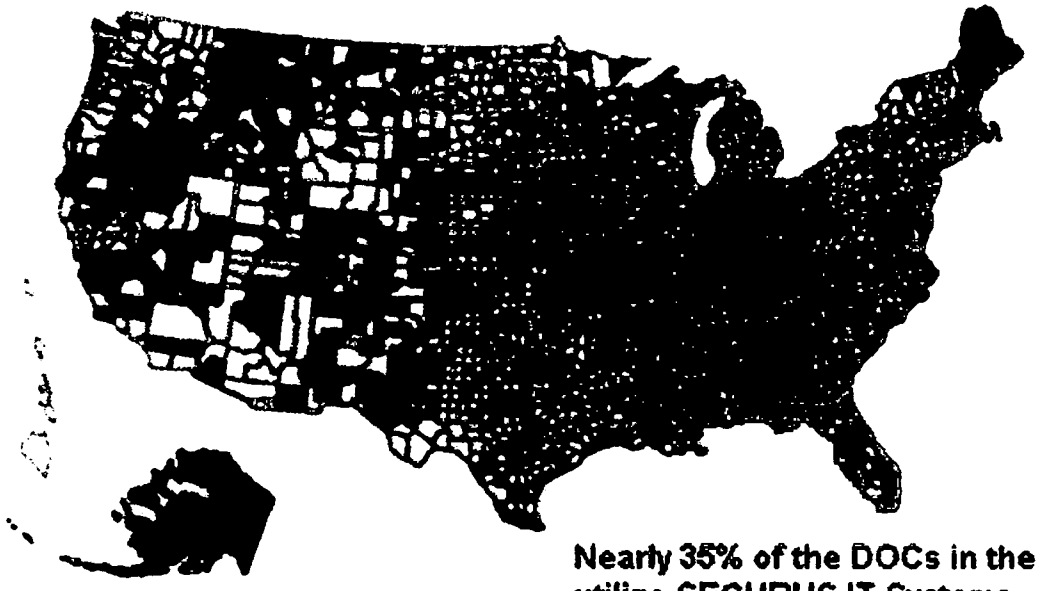
☑ **SECURUS has read and will comply.**

SECURUS is the largest independent provider of collect, pre-paid and debit calling services to local, county, state and private correctional facilities in the United States. SECURUS designs, implements and maintains inmate telecommunication systems and facility management software solutions that streamline the operation of criminal justice facilities and empower administrators with administrative, investigative and economic capabilities.

Our vast customer base allows SECURUS to keep a finger on the pulse of the Corrections industry, thus allowing us to identify trends in inmate calling and adapt to a constantly evolving Corrections telecommunications industry.

- **Currently installed in over 2,900 facilities nationwide.**
- **Over 500,000 DOC inmates at 17 DOCs are using SECURUS calling platforms.**
- **More than 40 Million Local and Long Distance inmate call transactions are being processed each month by SECURUS across 52,000 lines.**
- **Over 744,000 Inmates in other facilities are using SECURUS calling platforms (this includes County, City, Military, Federal, Private Prisons, Community Centers and Halfway Houses).**

SECURUS services correctional facilities in 49 states, including locations operated by city, county, state and federal authorities and other types of facilities such as juvenile detention centers and private jails.



Nearly 35% of the DOCs in the U.S. utilize SECURUS IT Systems

As you can see in the image above, SECURUS also has a significant operating base of US customers. By consistently offering unequaled expertise, superior service and application driven solutions, SECURUS has earned its place among the correctional industry's top telecommunications and information systems providers. Our sole focus is serving the highly specialized needs of the correctional industry and to continually strive to provide creative industry products and solutions to our customers.

References

North Dakota DOC
Tim Schuetzle, Director of Prisons
3100 Railroad Ave
Bismarck, ND 58501
(701) 328-6111
701.328.6640 (Fax)
Tschuetz@state.nd.us

Indiana DOC
Office of Information Technology
Greg Tuttle, Telecom Manager
Technology Services Division
302 West Washington
Indianapolis, IN 46204-2738
317.232.6933
317/232-5865 (Fax)
GTuttle@tsd.doc.state.in.us

Maryland DOC
Dayena M. Corcoran
Asst. Warden
Maryland DPSCS
MCI Women's
7943 Brockbridge Rd.
Jessup, MD 20794
(410)379-3803

TELUS Communications DOC
David Fowler, Director
3202-25 Avenue SW
Calgary, Alberta
Canada T3E0K6
(403) 530-4512
(877) 711-0111

Systems shall be capable of blocking toll free and other such numbers, third party calls, cell phone calls, call forwarding and specific numbers. **Lines must automatically disconnect if a third party call is detected.**

☑ **SECURUS has read and will comply.**

Call Blocking
During installation, a "Call Blocking" table is established which denies inmates from making calls to specific numbers. Access is denied to any number designated by the XXX.

The Secure Call Platform (SCP) is programmed to automatically prohibit calls to toll free, pay-per-call, directory assistance and emergency services, including: 800, 888, 877, 900, 976, 550, 555-1212, 700, 500, 911, 411, etc. Further, the Secure Call Platform automatically prohibit calls to all long distance carrier access codes including 10-XXX, 101-XXXX Primary Interstate Carrier (PIC) codes, all local numbers which access long distance carriers such as 950-XXXX and toll-free area codes and exchanges.

The Secure Call Platform has the capability to block virtually an unlimited number of calls at any one time. Number blocking is accomplished in one of three methods:

1. **Enter the number(s) to be blocked in the Restrict Number Editor through the on-site workstation, or**
2. **Submit the number(s) to be blocked to SECURUS**
3. **Our patented PERMAblock feature permits end users to have the capability of blocking their number via keystroke during call set up. This block will occur without Facility or SECURUS intervention.**

Either option provides for immediate restriction of the number once it is entered into the system. The Alaska DOC may submit a list of numbers they wish to have blocked and SECURUS will enter the numbers into the system prior to installation.

Call blocking can also be accomplished by the use of "wildcards". For example, using the NPA or NIP-NXX portions of the phone numbers, the system can be configured to block any number in the NAP or NPA-NXX range specified.

Because Call Blocking tables often contain thousands of entries, the Secure Call Platform offers virtually unlimited blocking potential with a capability of 10,000,000 individual entries. The entries may consist of an entire area code, an entire exchange code within an area code, or a specific telephone number.

This blocked number list may be administered locally by facility personnel using the Administrative Workstation, or remotely by the SECURUS National Service Center. All blocked numbers have an associated 'block' reason code that is stored in the blocked number database for future reference.

Additionally, the called party can use our patented PERMAblock feature to block their phone from receiving future calls by following the instructions of the voice prompts when the call is received and pressing the corresponding digit on their key pad to block their number.

3-Way Disconnect
SECURUS' inmate system will be capable of detecting and eliminating efforts to "transfer" inmate calls to a third party utilizing "3-Way calling" and/or "conferencing". Detection of any attempt by the called party to transfer an inmate call or to create a conference call will result in the call being immediately disconnected. As an option for investigative purposes the 3-Way call can be allowed to continue and be flagged. SECURUS' 3-Way and conferencing prevention feature(s)/technology are described below.

SECURUS will provide the Alaska DOC with the most robust and most effective switch-hook 3-Way call detection technology in the industry today. SECURUS is acknowledged as the undisputed leader in this field. Our research and development commitment has resulted in valued intellectual property, including the following 3-Way call detection patents:

- U.S. Patent #5,319,702 Methods and Apparatus for Detecting and Responding to Hook Flash Events Occurring on a Remote Telephone
- U.S. Patent #5,539,812 Method an Attempted 3-Way Conference Call on a Remote Telephone
- U.S. Patent #5,805,685 Three Way Call Detection By Counting Signal Characteristics
- U.S. Patent #5,796,811 Three Way Call Detection

An excellent example of our technological superiority is our continued development and perfection of 3-Way call detection. Around 1992, the introduction of 3-Way calling as a feature available by most local telephone companies created a problem for prisons and their need restrict inmates from accessing numbers the facilities had determined that should be blocked from inmate access. 3-Way calling also prevented prisons from having an accurate record of the inmate's telephone contacts, which created substantial security concerns. SECURUS, through our wholly owned subsidiary T-NETIX, was the first inmate call processing company to develop a solution to 3-Way calling using our now patented (US Patent Number 5,319,702) methodology.

Simply having the best 3-Way call detection in the industry was not enough for SECURUS. We have continued to research this issue and develop enhancements to our solution. Recent advancements in our 3-Way call detection methodology have led our customers to tell us they believe our 3-Way detection was operating nearly flawlessly. This led SECURUS to commission an outside firm in the 4th quarter 2006, SIBRIDGE consulting, an independent consultancy, to verify the accuracy of the 3-Way call detection feature.

The SIBRIDGE study collected and audited call recordings and event logs for approximately 6,000 calls. This independent test of our new 3-Way calling detection capability revealed SECURUS' overall success rate to be in the mid to high nineties, most significantly the system accurately detected and prevented illegal 3-Way call attempts 99 percent of the time.

The systems must be designed to provide inmates with a "PIN" number assignment. The system must also provide for exclusion of "PIN" number assignments to pre-trial detainees.

☑ **SECURUS has read and will comply.**

Call duration, phone usage times, and voice prompts language features may all be programmed at the individual inmate level. Each inmate telephone may be programmed for PIN or non-PIN operation.

Some inmate facilities may choose to operate using a PIN system, under which each inmate is assigned a personal identification number (PIN). The inmate then needs to enter his or her PIN before allowed to make a telephone call. PINs also provide an audit trail of the specific inmate that placed a specific call. Additionally, it allows the facility to allow or deny telephone numbers based on inmate identity.

Each inmate is assigned a unique Personal Identification Number (PIN), ranging anywhere from four (4) to sixteen (16) digits. This range creates a maximum number of nine (9) billion PIN combinations. The system has the ability to randomly generate PINs and automatically assign PINs to the inmate.

This traditional method of creating Approved Calling Lists provides the most restrictive type of calling privileges, including an approved calling list with a

minimum of twenty (20) numbers for each PIN. The facility will determine the maximum number of telephone numbers each inmate is allowed to register. Registration of a telephone number includes the number, name of the party who the inmate wishes to call, and the relationship of that party to the inmate. The telephone numbers registered by each inmate are identified with the inmate's PIN and are resident in the system.

Below are the three primary modes, which may be applied to a single phone or group of phones in a facility:

Mode 1 – Open PIN
This is the most basic mode of operation and the simplest to administer. Each inmate is assigned a unique PIN that will be required to make a phone call; however, no individual phone number restrictions or calling lists are utilized in this mode. Only global system calling restrictions will be applied to the inmate's calls.

Mode 2 – Open PIN with Restrictions
Mode 2 builds on the Mode 1 Open PIN feature and adds the ability to place restrictions and limits on specific phone numbers, while allowing all other phone numbers to be processed as they would in an Open PIN system. Mode 2 restrictions can also include the recording and alarming of numbers, language options, special parameters for destination numbers, and the use of facility or global number lists.

Mode 3 – Closed PIN
Mode 3 provides the most restrictive type of calling privileges; however, it is also the most administration-intensive of the three modes. In the system's standard configuration, each inmate is allowed to register from one (1) to twenty (20) telephone numbers. The total number of destination numbers available to put on an inmate's list is unlimited. The facility will determine the maximum number of telephone numbers each inmate is allowed to register. Registration of a telephone number includes the number, name of the party who the inmate wishes to call, and the relationship of that party to the inmate. The telephone numbers registered by each inmate are identified with the inmate's PIN and are resident in the system. Only that specific PIN may validate calls to those numbers.

Pre-Trial Detainees
The system will also allow groups of phones, such as the phones for the pre-trial detainees, to operate without the use of PINs.

AutoPin
SECURUS can provide an interface with Alaska DOC's offender management system, which will provide for the facility to choose a number from the offender management system to be used as the PIN for the inmate phone system. This number and inmate number will automatically be entered into the phone system upon the inmate being booked into the facility.

Different voice announcements must be provided for inmate and pre-trial detainees.

☑ **SECURUS has read and will comply.**

The SECURUS Secure Call Platform provides customized professionally recorded voice prompts allowing for specific call progressions and requirements. Personalized prompts can be assigned to a facility, group of telephones or PIN identifying the inmate or facility classification on each attempted call.

Systems shall have the ability to limit the duration of inmate and pre-trial detainee calls with a notification of time limit at points three minutes, one minute, and 30 seconds before conclusion. Exceptions will be made in the case of attorney calls.

☑ **SECURUS has read and will comply.**

With SECURUS' calling platform, inmate call duration is completely programmable and may be limited to a specific time interval, e.g. 15 minutes per call. The time limit may be changed for each active line, individual inmates, and/or the entire system. Additionally, the Alaska DOC can choose to limit the number of calls per day or week, hours during which calls can be made, and the type of calls that can be made during each time period.

A verbal warning can be given at three (3) minutes, one (1) minute, and thirty (30) seconds before the end of the programmed time interval, indicating that the call will be terminated. This feature is also programmable. Both the inmate and the called party are notified of call termination by voice prompting at one minute prior to the end of the call's pre-programmed time limit. By assigning a different Class of Service (COS), call termination notification may be disengaged for specific numbers such as attorney's numbers, public defenders, etc. All call records contain a 'reason for termination' code that indicates why a call ended.

The systems must prevent dialing a second number after a called party hangs up.

☑ **SECURUS has read and will comply.**

The proposed system constantly monitors the hookswitch of the inmate telephone. If the hookswitch is depressed at any time, internal dial tone will reappear. This prevents hookswitch manipulation for fraudulent purposes and prevents dialing if secondary dial tone is received after the called party hangs up.

Should an on-hook transition be missed by the proposed ITS, the system continuously looks for the occurrence of DTMF tones and dial tone. After proper timing qualification of these tones, to prevent inadvertent disconnects due to ambient background noise, the system will cause call termination resulting in the re-establishment of either PIN tone, or dial tone to the inmate, forcing a new, fully-controlled call.

This will be a "turn-key" system. On site training must be provided for all operators of the inmate phone system. Such training must include operation and first echelon maintenance of all equipment supplied.

☑ **SECURUS has read and will comply.**

SECURUS is the current provider of the Alaska DOC inmate calling system known as CAM. Our offer includes the installation of all new equipment to the latest generation of the SECURUS Secure Call Platform (SCP). This upgrade will be a "turn-key" installation. All additional wiring, cabling, conduit, cross-connects, jacks, plates and related hardware, necessary for the operation of the system shall be provided at no cost to the Alaska DOC. SECURUS assigns fully qualified, factory trained field technicians to install and maintain the Secure Call Platform for the duration of the contract period.

SECURUS provides thorough training on the operation of the Secure Call Platform and its user utilities. Each session is customized to meet the experience and expertise level that best suits the attendees. Training sessions may be conducted regionally or individually (by institution), as determined by the Alaska DOC. The number of attendees per session is dependant upon the availability and size of the room where the training is held. There is no maximum number of people that can attend the sessions. Sessions typically last 2-4 hours; however, the sessions will not end before attendees have a thorough working knowledge of the system and its components. Follow-up training is also provided as needed. This training can be done via Web Cast, on-site visit, or remotely by taking "control" of the system and walking the administrator through the steps necessary to complete their task(s).

Acceptance testing shall be performed at each facility in the presence of DOC personnel and/or their designated representative.

☑ **SECURUS has read and will comply.**

General Offeror Requirements:

5.02.1 The Offeror shall establish an internal "Account Team" to interface with DOC for the ITS. This Account Team will serve as the single-point-of contact (SPOC) for DOC and shall provide new telephones, system and network design services, system programming services, system transition and implementation services, post installation programming, updates and maintenance services and commission fee schedule services.

☑ **SECURUS has read and will comply.**

The SECURUS Account Team members will provide a single-point-of contact for the Alaska DOC for all services related to the ITS. The SECURUS Account Team will be available to meet monthly with Alaska DOC's staff for the purpose of presenting monthly maintenance and administrative reports. Annual Alaska

DOC reviews and technology roundtable updates are scheduled and conducted with the Alaska DOC staff.

The Offeror shall provide access to the Account Team in the following manner:

A. By voice telephone number and facsimile transmission
B. By toll free 800/888/877 numbers for telephone and facsimile access.
C. By E-Mail (Internet) address.

☑ **SECURUS has read and will comply.**

SECURUS' Alaska DOC Account Team:

Kevin Collins, Account Executive	**Telephone: 720-488-5696**
	FAX: 972-277-0301
	Toll Free: 800-844-6591
	Email: kcollins@securustech.net
Helen McCoy, Project Manager	**Telephone: 231-258-4971**
	FAX: 231-258-4971
	Toll Free: 800-559-1535
	Email: hmccoy@securustech.net
Jason Kintner, Field Technician II	**Telephone: 907-227-4873**
	FAX: 972-277-0301
	Toll Free: 800-559-1535
	Email: jkintner@securustech.net

5.02.2 DOC reserves the right to reject personnel assigned to the Account Team including personnel from the Contractor and personnel from any subcontractors during the life of the contract.

☑ **SECURUS has read and will comply.**

5.02.3 The Account Team shall work in conjunction with any Customer Premise Equipment (CPE) or network contractor (voice or data) being used by DOC to resolve any technical problems that may arise between the proposed ITS system and any existing or future voice/data systems installed by DOC. This will eliminate the need for DOC to be a mediator in problem resolutions. Upon request of DOC, the Account Team shall speak directly with any other CPE contractor, local exchange carrier, long distance carrier, etc. to resolve technical issues.

☑ **SECURUS has read and will comply.**

5.02.4 The Offeror shall adhere to any municipal, state or federal requirements for ITS installation "certification", training, or registration. Failure to comply with present and future municipal, state or federal requirements may result in termination of any Contract with the Offeror and the paying of any applicable fines, etc. incurred by DOC for violation of such requirements by the Offeror,

☑ **SECURUS has read and will comply.**

The Offeror shall be responsible for compliance with all regulatory requirements imposed by local, state and federal regulatory agencies for all systems and services provided throughout the duration of the Contract.

☑ **SECURUS has read and will comply.**

5.02.5 The Offeror's Account Team must accept system programming and maintenance orders only from authorized personnel with the DOC. The Account Team must determine authorized personnel as part of their Proposal's initial contracting process and provide authorization forms for agency personnel signatures. The Offeror will be responsible for all charges associated with "unauthorized" service repairs, additions, or changes performed by the Offeror.

☑ **SECURUS has read and will comply.**

SECURUS is the current provider of the Alaska DOC inmate calling system providing no cost maintenance of all installed equipment and will continue to do so if selected as the preferred vendor for the next contract term. Our offer includes the installation of all new equipment to the latest generation of the SECURUS Secure Call Platform (SCP). All components of the installation including any additional wiring, cabling, conduit, cross-connects, jacks, plates and related hardware, necessary for the operation of the system shall be provided and maintained at no cost to the Alaska DOC. SECURUS assigns fully qualified, factory trained field technicians to install and maintain the SCP for the duration of the contract period. Upon award, the SECURUS Account Team will provide all necessary authorization forms for authorized agency personnel signatures.

5.02.6 The Offeror shall be responsible for making all system modifications necessary to allow inmates to place calls as industry dialing requirements change at no cost to DOC. Such modifications must be made in a timely manner to ensure proper use of the ITS system by inmates and DOC personnel.

☑ **SECURUS has read and will comply.**

5.02.7 The Offeror shall be responsible for complying with and updating the ITS for any regulatory changes and requirements during the life of the contract. These regulatory changes include federal, state or local municipal modifications. These changes must be made in a timely manner and at no cost to DOC.

☑ **SECURUS has read and will comply.**

5.03
General Inmate Telephone System Requirements

The proposed ITS shall be provided for all DOC facilities, listed in Table 1 of this RFP at no cost to DOC for installation, training, operation and maintenance of the ITS, equipment, software, and its components. If the ITS system is damaged or destroyed, the Offeror is responsible for replacement of the ITS system in its entirety or its individual components regardless of cause including, but not limited to, normal wear/use, inmate abuse, natural disaster, or inmate unrest. The ITS system or component replacement shall be performed at no cost to the DOC. The Contractor owns the ITS equipment. The ITS proposed for DOC must meet or exceed the following requirements:

☑ **SECURUS has read and will comply.**

5.03.1 The ITS proposed for DOC shall include the following components:

A. A Site/Location Call Processor-Control System located at each DOC facility listed in Table 1.

☑ **SECURUS has read and will comply.**

B. A Centralized System Database.

☑ **SECURUS has read and will comply.**

SECURUS' has a centralized data center in Allen, Texas, a secondary data center in Dallas, Texas and a Disaster Recovery data center in Irving, Texas. These three data centers provide SECURUS with both site-level and server-level redundancy. SECURUS recently completed the process of building a regional data center to support the Secure Call Platform infrastructure in Atlanta, Georgia. Additional sites are being reviewed if the need arises.

Each remote site can be connected to a central site using SECURUS-provided bandwidth. This connectivity provides a data link from the remote platforms to the central site for transferring call records and user profiles. Call records are generated centrally and reports and data can be retrieved from remote sites. New or updated user profiles and system configuration data are managed centrally through the Secure Call Platform and can be updated by authorized users at any site. Authorized users from any sites have the ability to securely login to operate the system, change system configuration, troubleshoot, and retrieve data. The system's security features at both the central site and each remote site strictly control this operation. System operators must have a security clearance based on passwords, user –IDs, and security levels to gain access to any individual features of the proposed ITS.

C. Recording and Digital Monitoring Equipment.

☑ **SECURUS has read and will comply.**

Call Monitoring
The Secure Call Platform Live application allows for immediate, real-time monitoring of calls in progress via the multi-media PC workstation. Facility personnel (with appropriate password privileges) are able to monitor live calls by simply highlighting the call in progress and clicking on the speaker icon. This process is undetectable by either the inmate or the called party and does not disrupt the recording process. Furthermore, concise descriptions of activity are displayed for each phone in use, for example, the system displays the specific telephone location, inmate PIN and name (if option is used), the destination number dialed, city and state of the destination, time and duration of call, any restrictions such as "Watched" or "Private", and the status of the call, such as "In Progress," "Calling Destination," "Get Acceptance".

The system also provides the ability to automatically eliminate any monitoring or recording of special calls, such as to legal counsel, by designating the number as a "private" number. In the event that a retrieval of a "private" call is attempted, the Secure Call Platform will inform the user that, "This call is prohibited from monitoring."

Call Monitoring, Silent
When monitoring is invoked, the system incorporates analog suppression/ amplification hardware that allows correctional officer monitoring of calls without inmate or called party detection. There is absolutely no noise, dB loss or other indicator when this feature is activated via handset, headset or amplification instrument (speakerphone, orator, magnetic, taping equipment, etc.).

Call Recording
The Secure Call Platform's unique, fully integrated recording application, works independently of other product(s) so there is never a need for separate manufacturer's product to work along side the system. The Secure Call Platform employs large capacity hard drives along with RAID (Redundant Array of Inexpensive Disks) that virtually extend the call storage period and enhance system redundancy and call backup to meet your specific needs. With the Secure Call Platform, all calls are maintained on-site for easy access when immediate retrieval of information is critical to your investigative team.

The Secure Call Platform can also burn the information to CD and/or DVD for additional back up, if necessary.

The Secure Call Platform is capable of recording all calls simultaneously and also allow personnel to listen to a pre-recorded call, while active calls

continue to be recorded—all without loss of information. The system records the entire conversation from the time the inmate lifts the handset off the cradle to termination of the call. Because the recording and monitoring applications are fully integrated features of the system, call synchronization between call record time and recording time is guaranteed.

Simultaneous Recording
The Secure Call Platform is capable of recording all calls simultaneously and also allows personnel to listen to a pre-recorded call, while active calls continue to be recorded—all without loss of information. The system records the entire conversation from the time of positive acceptance to termination of the call.

Remote Call Forwarding and "Hot Number" Alert
The system is equipped with a remote call-forwarding feature for those numbers that are under surveillance by the investigative unit. The Covert Alert feature allows authorized personnel to monitor a call, from any designated remote location, while the call is in progress. Once a number, or PIN, is assigned a 'covert' status, the user simply enters a telephone number (cellular, home, office, etc.) to which he/she wants the call sent for 'Live' monitoring. The call is then automatically re-routed once the call is accepted by the called party and in progress. There are no distance barriers to the retrieval process so the remote telephone number can be located within the facility or across the country. As an additional benefit, administrators may continue to monitor other calls, through the on-site workstation, while utilizing the 'Covert Alert' remote live call-forwarding feature.

Call Playback and Copying
The call playback feature will allow 360 days of recorded calls for immediate retrieval and allow search and playback within 30 seconds. Corrections personnel can listen to live or archived recordings via multi-media PC interfaces connected over Local Area Networks. Multiple levels of security provide that only authorized personnel can access and monitor the inmate recordings. The audio may be directed to the integrated loudspeaker or headphones. This output may be also be used to record the conversation(s).

Recordings are played back using the SECURUS media control, accessible through the SECURUS Web Portal and can then be stored to CD as needed by the Alaska DOC.

The SECURUS Secure Call Platform provides the capability to copy the conversations onto a compact disc (CD) or other storage device. Administrative terminals will be equipped with speakers and a CD R/W device to comply with this request.

accessing the numbers that would normally be blocked such as victims or witnesses. SECURUS' patented 3-Way Call Detection provides a proven, patented technology that performs at the highest success rate in the industry. No other vendor can claim a proven, patented solution for this most common fraud type. Our technology prevents telephone abuse and harassment of witnesses and other parties involved in criminal prosecution and protects the community from fraudulent, threatening, or harassing calls. Our technology team has just deployed an enhanced 3-Way Call Detection process that is providing extremely precise detection of 3-Way Call attempts and we have eliminated the ability of the inmate to mask the 3-Way Call attempt by corrupting the channel though noise diversion, such as blowing into the phone handset during the 3-Way attempt.

SECURUS will provide the facility with the most robust and most effective switch-hook 3-Way call detection technology in the industry today. SECURUS is widely acknowledged as the undisputed leader in this field. Our research and development commitment has valued intellectual property with the following 3-Way Call Detection patents:

- U.S. Patent #5,319,702 Methods and Apparatus for Detecting and Responding to Hook Flash Events Occurring on a Remote Telephone
- U.S. Patent #5,539,812 Method an Attempted 3-Way Conference Call on a Remote Telephone
- U.S. Patent #5,805,685 3-Way Call Detection by Counting Signal Characteristics
- U.S. Patent #5,796,811 3-Way Call Detection

SECURUS' patented 3-Way Call detection feature has been proven in independent tests to have nearly flawless effectiveness.

With all 3-Way call blocking methods, the technology requires "art" as well as science. Its configuration at each facility will be customized by SECURUS to adjust sensitive parameters and thresholds for optimum performance.

The 3-Way Conference Calling Fraud Detection feature prohibits the major fraud practice possible with other automated and live-operator systems. Inmates could enlist the aid of an outside accomplice to "conference" them, via Central Office-provided 3-Way calling, to an "unrestricted" line, bypassing the system controls. Without this protection, inmates have in effect, unrestricted access to the outside world, defeating the correctional objectives and policies of the institution along with subjecting the public to inmate harassment and fraud. SECURUS' system is unique in its ability to detect and foil an accomplice's attempt to activate the 3-Way call

Recorded calls can be transferred to a CD via the CD Burner function of the Secure Call Platform. There are three choices for CD format. Data CD is automatically selected, but you can select Data CD Encrypted requiring a password to play back a call or Audio CD for playback on any portable CD player.

Data CD—allows approximately 2,900 minutes to be saved to the CD. In addition to the call recordings, a program is saved to the CD that allows playback from any computer.

Audio CD—allows approximately 80 minutes of calls to be saved to the CD. This CD plays just as any audio CD.

D. Ability to interface with competitors systems.

☑ **SECURUS has read and will comply.**

SECURUS has successfully integrated hundreds of customers throughout dozens of applications including Offender Management Systems and Commissary companies with automation functionalities to help their facilities become more efficient and cost effective.

SECURUS works with companies such as Syscon and others to establish a reusable interface to automate items such as PIN integration, debit account management, data gathering and information sharing capabilities.

E. Web based access.

☑ **SECURUS has read and will comply.**

SECURUS' system is web-based, and authorized personnel can manage the system and review data from any location with internet access. The system is fully administrable either on-site or remotely.

SECURUS' S-Gate Portal opens a secure window into a facility's operations providing authorized personnel with the access to an array of applications' functions and modules that are design to aid correctional facility to maintain safe and efficient operations. Whether you investigate inmates' potentially fraudulent activities, require technical support or inquiring the status of the commission check, the information is at your fingertips and available 24 hours a day 365 days a year.

F. Three way call detection.

☑ **SECURUS has read and will comply.**

While it is true that 3-Way Call Detection provided by other vendors may be an imprecise technology that does not prevent inmates from

feature by immediately disconnecting the call upon detection. SECURUS' proposed ITS has the unique ability to disable 3-Way call detection on a particular number or groups of numbers, such as attorneys.

Selective Programming
Additionally, our 3-Way detection feature can be enabled according to classes of service, meaning facilities can choose whether to employ 3-Way prevention globally, or they can disallow 3-Way calling for specific phones, groups of phones or PINs.

G. Key word or phrase search capability.

☑ **SECURUS has read and will comply.**

SECURUS offers a keyword or phrase search turnkey solution for correctional facilities' recorded inmate conversations. This technology assists investigators in searching inmate conversations for words or phrases such as trigger words associated with potential escape scenarios and drug-related incidents. This solution makes it possible for the investigators to search for and replay specific words or phrases within audio recordings. This productivity tool significantly expedites audio searches, which are highly time-consuming using traditional retrieval methods that require listening to extended portions of recordings to locate desired content.

Word search provides fast and easy navigation of audio files, and is far superior to the rudimentary "start" and "stop" functions of conventional media player controls. The user can quickly locate specific words and phrases that match their search request, then click and play back the desired audio content. In addition, it provides advanced language processing features such as "sounds like" searches, and generation of a list of the key topic words spoken in a specific recording.

While this application is not foolproof, it adds a significant tool to help investigators save valuable time and solve crimes.

5.03.2 The Offeror shall propose one type of ITS for all DOC locations. All system hardware, software and support systems shall be the same in each DOC facility.

☑ **SECURUS has read and will comply.**

5.03.3 The Site/Location Call Processor shall provide for all telecommunications capabilities for inmate services as well as administrative capabilities for DOC personnel.

☑ **SECURUS has read and will comply.**

The SECURUS Secure Call Platform is a highly featured, state-of-the-art system designed to provide the Alaska DOC with the ultimate in inmate call control and reporting. The advanced features of the system provide extremely powerful and flexible tools for controlling inmate calling, reducing fraud, and generating valuable administrative reports.

SECURUS' custom built Secure Call Platform (SCP) is an integrated platform of software tools and computer and telephony hardware. The Secure Call Platform's hardware and software components are designed to adapt to the changing needs of a facility's operations. The Secure Call Platform is capable of real time inmate telephone monitoring, inmate telephone recording, call blocking/unblocking, and report generation.

Scalable and flexible, the system's hardware and software components are designed to adapt to the changing needs of a facility's operations.

The Secure Call Platform allows staff and investigators the ability to maintain security through a reliable and easy-to-use inmate call control system. The Secure Call Platform provides security to the public through the use of automated operators instead of live operators, the use of Personal Allowed Number (PAN) lists that do not allow calls to numbers that have not been approved by the system administration, the use of inmate call monitoring and recording for investigative and safety purposes, the use of call duration settings and telephone on/off times, the use of call detail records for investigative purposes, and fraud control features.

The Secure Call Platform is equipped with the following standard applications:

- Digital Recording and Playback (accessible and installed if found necessary)
- Dedicated Customer Care Center to specifically address called party inquiries
- A variety of optional calling methods and platform flexibility to increase options and income for the facility while increasing inmate's calling ability
- Number Restriction/Blocking Capabilities
- Identification of watched numbers, attorney calls (Private) on CDR
- Multi-level password security entry system and each application
- Call Detail Reports based on user search criteria
- Inmate Accounting package for prepay calling and commissary ordering
- PIN Application with Personal Allowed Number (PAN) list capabilities
- Voice technologies to enhance system controls and investigative qualities

- **Expanded fraud control features (3-Way, additional digit dialing, etc.)**
- **Bilingual automated voice messaging, instructional prompts, tag lines and voice overlays**
- **Fully integrated debit-based calling platform**
- **Interface and integration capabilities**
- **Immediate port disabling**
- **Automated PIN and PAN assignment**
- **Remote live monitoring capabilities—anywhere nationwide**
- **True call portability for replay of conversations without Secure Call Platform software**

5.03.4 The Centralized System Database shall be located at a Offeror provided site, located outside of DOC facilities but within the Central or Western United States, and provide full database redundancy for all Site/location Processors and recording equipment at each DOC facility (see Section 5.3).

☑ **SECURUS has read and will comply.**

The redundancy built in to the SECURUS system effectively prevents loss of data and system downtime because all of the data is stored in an offsite, centralized database and backed up at multiple locations across the nation. Because the system is web-based, the data can be accessed at any location with an internet connection, and SECURUS' Secure Connect Architecture maintains the system at the highest level of operability.

In addition, all call records will be duplicated and backed-up at two fully-staffed data centers in Allen and Dallas, Texas. Each data center comprises two fully redundant systems, each with its own circuit feed, its own physical racks, redundant communication, redundant termination carriers, and redundant A&B power with UPS and generator backup. The physical storage itself is also advanced; the data is stored via both SAN and robotic tape, and the data centers are connected to one another by a Metropolitan Area Network Ring. Additionally, the system features full state awareness of each call with the ability to fail over to another data center if necessary, in most cases without dropping the call in progress.

5.03.5 The ITS shall be provided to DOC at no cost. The ITS proposed for DOC shall include full design, installation and on-going maintenance and repair and replacement at no cost to the DOC.

☑ **SECURUS has read and will comply.**

5.03.6 The ITS shall provide any network services as specified in this RFP, at no cost to the DOC, during the duration of the Contract.

☑ **SECURUS has read and will comply.**

5.03.7 The ITS shall allow inmate access to collect and prepaid call services as described in this RFP document. At no time would inmate telephones be allowed to make calls without some type of ITS system restriction and monitoring (with the exception of those that qualify as attorney/client privileged calls).

☑ **SECURUS has read and will comply.**

5.03.8 The ITS shall allow for all inmate telephones to be in use simultaneously. Dial tone shall be presented immediately to all inmate telephones in an "off hook" position. There shall be one central office line per inmate telephone. **All lines must be provided at no cost to DOC.**

☑ **SECURUS has read and will comply.**

5.03.9 The call automated announcement function of the ITS shall be capable of processing calls on a selective bilingual basis. The inmate shall be able to select the preferred language using no more than a two-digit code.

☑ **SECURUS has read and will comply.**

The proposed system is capable of providing message prompts in English and Spanish. An inmate may select a specific language at the beginning of the call process by dialing a single digit. This will initiate the selected language prompts to the inmate. If desired, the language selection for the called party may be preset in the system database. If additional languages are required, they may be developed for specific customer needs at no cost.

5.03.10 The Offeror shall propose an ITS that can be shut down immediately and selectively. DOC shall be able to shutdown the ITS system globally and restrict all PIN access, within an entire facility and/or within a facility wing. The Proposal shall describe the options available to DOC for this type of immediate and global restriction.

☑ **SECURUS has read and will comply.**

Manual Shutdown
The entire phone system or individual phones or groups of phones may be turned On/Off with a few clicks of the mouse at the on-site workstation and/or manipulated by toggle switches located in a secure location of the facility(ies).

The Phone Cut-off Switch form of manual control allows facility personnel to disable a certain phone or groups of phones in an out of service condition. While this function can be performed through the administrative terminal, the site is also equipped with these manual cut-off switches located in the section

command control room. In the event of an uprising, this SECURUS feature prevents inmates from reaching assistance outside the facility.

Selective Restrictions
Many restrictions may be tagged to any PIN or telephone number associated with a PIN.

Examples of restrictions are:

- **Time of day and/or days of week that a number may be called**
- **Maximum duration of a call for that number and/or PIN**
- **Maximum number of calls to that number or from that PIN per day/week/month/amount, etc.**

When restrictions are imposed, they are automatically managed by the calling platform.

5.03.11 The proposed ITS shall be restricted to outgoing calls only. The ITS shall not process incoming calls at any time. No inmate telephone shall be capable of receiving an incoming call and Offeror shall work with the local telephone companies to ensure such control. The Proposal shall describe how this component shall be achieved for the DOC.

☑ **SECURUS has read and will comply.**

The SECURUS calling platform allows for outgoing, collect or pre-paid debit calling only. At no time can incoming calls be received. It is our standard procedure to install telephone lines or circuits that are configured to prohibit incoming calls. The system is configured to busy all trunks that receive ring voltage associated with an incoming call. This eliminates the possibility of a facility receiving incoming calls on the inmate system. SECURUS works with all local exchange carriers to ensure this. The telephony controllers utilize extensive security measures to insure that inmates cannot receive incoming calls from parties either within or outside the facility.

5.03.12 The Offeror shall keep all call processing and call rating information current. This information includes, but is not limited to, local exchanges, area codes, country codes, vertical and horizontal coordinates and any other information necessary to accurately process and rate calls. The Offeror must quickly provide DOC with any rate information for all calls upon request by DOC at any time during the term of the Contract.

☑ **SECURUS has read and will comply.**

5.03.13 The ITS shall block all calls made to any telephone numbers that incur excess charges such as 900, 972: 976, 550, etc. The Offeror shall be responsible for ensuring that the ITS System is programmed for such blocking.

☑ **SECURUS has read and will comply.**

The Inmate Calling System will by default prohibit calls to toll free, pay-per-call, directory assistance and emergency services, including: 800, 888, 877, 900, 972, 976, 550, 555-1212, 700, 500, 911, 411, etc.

Authorized personnel with appropriate secure access can modify the allowed/disallowed number list at any time.

5.03.14 The ITS shall block all inmate calls to current long distance carrier access numbers (i.e., 101 0333 and 101 0285) or future 101-xxxx carrier access numbers. The Offeror shall be responsible for ensuring that the ITS system is programmed for such blocking.

☑ **SECURUS has read and will comply.**

The system automatically prohibits calls to all long distance carrier access codes including 10-XXX, 101-XXXX Primary Interstate Carrier (PIC) codes, all local numbers which access long distance carriers such as 950-XXXX and toll-free area codes and exchanges.

Authorized personnel with appropriate secure access can modify the allowed/disallowed number list at any time.

5.03.15 The ITS shall block all local numbers that access long distance carriers. The Offeror shall be responsible for ensuring that the ITS system is programmed for such blocking.

☑ **SECURUS has read and will comply.**

5.03.16 The ITS shall block all inmate access to directory assistance access numbers (i.e., 411, 555-1212). The Offeror shall be responsible for ensuring that the ITS is programmed for such blocking.

☑ **SECURUS has read and will comply.**

The Inmate Calling System will by default prohibit calls to 411, 555-1212, etc.

5.03.17 The ITS shall block all inmate access to toll free numbers (i.e., 800, 888 and 877). The Offeror shall be responsible for ensuring that the ITS is programmed for such blocking. The ITS must have the capability to allow the DOC to unblock individual toll-free numbers.

☑ **SECURUS has read and will comply.**

The ITS will block all inmate access to 800, 888, 877, etc.

With SECURUS' system, administrators can enter specific allowed numbers into the database that will override the global blocking of toll-free numbers.

The system has the ability to assign unlimited allowed or blocked numbers per PIN. These allowed/blocked numbers will override the Global allowed/blocked call table and be unlimited in amount.

5.03.18 Offeror shall insure that local calls are not passed off to any other carrier not authorized by the Contract. This will include call forwarding from a local AN1 to any of the lists of numbers required to be blocked or automatically forwarded to numbers not dialed directly by the inmate. The Offeror is authorized by the Contract to have exclusive control over all billing of local, intraLATA, interLATA and international long distance collect and prepaid calls placed by inmates through the ITS.

☑ **SECURUS has read and will comply.**

The patent pending RCFD process proactively detects calls to telephone numbers that have been automatically forwarded by called parties. These numbers are forwarded through the use of local or toll free numbers provided by 3rd party telecom service providers. This patent-pending screening process gives facilities control over possible RCF activity. Without proper detection, RCF activity often results in;

- **Decreased revenue from long distance arbitrage (calls which should have been rated as long distance are transitioned to locally rated calls)**
- **Decreased security and increased liability by allowing inmate's access to unauthorized individuals (i.e., victims, judges, etc.)**
- **Increased exposure to called parties non-payment of calls**

5.03.19 The ITS shall be capable of interfacing with network services provided by local exchange carriers as well as inter-exchange carriers. This includes analog and digital facilities (i.e., analog business trunks, DS-I, and ISDN PRI). The Proposal shall state the types of network services to which the proposed ITS will interface and the purpose (application) of such services for DOC.

☑ **SECURUS has read and will comply.**

All Calling Platforms provided by SECURUS interface with industry standard Analog and Digital provisioned circuits such as POTS, ISDN, PRI, T-1/DS-1 and DS-3 services. The trunks to be provisioned for the Alaska DOC will be Primary Rate Interface (PRI) T-1's known by the industry as smart trunks. The PRI's provide detailed information for advanced call routing, call progress and enforce outgoing service only.

Remote diagnostics, analysis, and monitoring of the Secure Call Network (SCN) are performed by Sentinel. Sentinel is SECURUS' system and networking monitoring package that proactively alerts technical personnel of irregularities in the system software and hardware. The system maintains connectivity to the SCN over the Wide Area Network. Sentinel continually monitors key trouble areas and automatically assigns service consultants and/or dispatches field

technicians to insure optimal operation of your system 24/7. Sentinel actively monitors communication channels, CPUs, disks, messages, processors and servers to insure optimal operations at all times.

Sentinel is available from the SECURUS secure MPLS network and authorized Alaska DOC personnel will receive an access link. Each indicator is polled once every five minutes to determine its status.

5.03.20 The Offeror shall describe the type of network services it will provide with the proposed ITS.

☑ **SECURUS has read and will comply.**

The type of trunks connecting all calls to the Public Switched Telephone Network (PSTN) offered as part of this contract will primarily be Digital Primary Rate Interface (PRI) T-1's. PRI's are used for Integrated Services Digital Network (ISDN) applications and has 23 B-channels and 1 D-channel per T-1. The B channels are generally used for voice and/or data traffic while the D channel maximize the use of the B channel as well as providing advance call routing services for Local, Long Distance and International calling destinations.

5.03.21 It is the intention of the DOC to initially implement the proposed ITS in a collect call and prepaid calling modes. Collect calling shall be offered for all 50 states and United States territories.

☑ **SECURUS has read and will comply.**

5.03.22 The Offeror shall implement an ITS that provides telephone reception quality meeting all industry standards for service quality as defined by the Regulatory Commission of Alaska (RCA) and by the Federal Communications Commission (FCC). The Offeror shall accept the DOC's judgment concerning these standards.

☑ **SECURUS has read and will comply.**

SECURUS provides P.01, or better, level of service. SECURUS utilizes state-of-the-art electronic equipment, and digital recording and T1 equipment to provide acceptable audio quality, at a minimum. SECURUS does not use voice compression, and maintains an audio frequency response of +/-.1dB, 300-3400Hz (relative to 0 dBm, 1000Hz). Extensive testing is performed, including numerous test calls from each facility during installation, to ensure excellent audio quality and dial tone availability.

A P.01 Grade of Service (GOS) is "the probability (P), expressed as a decimal fraction that one call out of one hundred, during the average busy hour, will be blocked. "It is in the best interest of SECURUS to complete as many calls as possible. Therefore, all systems have immediate automated reporting that shows when a call was unable to be completed due to a busy condition. In the

event call traffic increases and the GOS falls below P.05, SECURUS will install additional lines to the Calling Platform at no cost to the State.

5.03.23 The proposed ITS shall provide that "call set-up time" not exceed 10 seconds from completion of dialing to first ring.

☑ **SECURUS has read and will comply.**

"Call set-up time" will not exceed ten (10) seconds from completion of dialing to first ring.

5.03.24 The proposed ITS shall not provide a second dial tone to an inmate telephone without the inmate hanging up the telephone receiver after the first call is completed.

☑ **SECURUS has read and will comply.**

The system does not allow an inmate to obtain a second dial tone without termination of the first call. Follow-on, or "chain" dialing, is prevented by a combination of features. When the called party disconnects prior to, or without the inmate hanging up, the Public Switched Telephone Network (PSTN) should by today's standards not return a "second" dial tone. Instead, a pre-recorded message such as "If you would like to make a call, please hang up then place your call," will be played to the inmate. Since not all Local Exchange Carriers implement this standard, the system uses the SECURUS patented 3-Way Call Detection System, plus standard battery, dial tone, and DTMF detection, to detect the called party's on-hook condition.

The system constantly monitors the hookswitch of the inmate telephone. If the hookswitch is depressed at any time, internal dial tone will reappear. This prevents hookswitch manipulation for fraudulent purposes and prevents dialing if secondary dial tone is received after the called party hangs-up. Should an on-hook transition be missed by the system, the system continuously looks for the occurrence of DTMF tones and dial tone. After proper timing qualification of these tones, to prevent inadvertent disconnects due to ambient background noise, the system will cause call termination resulting in the re-establishment of either PIN tone, or dial tone to the inmate, forcing a new, fully-controlled call

5.03.25 The proposed ITS shall allow for an agreed to "ring time" before an inmate call is disconnected. This "ring time" parameter shall be programmable by DOC but shall be consistent among DOC facilities.

☑ **SECURUS has read and will comply.**

5.03.26 The proposed ITS shall provide notification to an inmate of the call status (i.e., ringing and busy). This notification may either be in the form of ringing, busy tones, standard information tones (SIT), or appropriate recorded messages.

☑ **SECURUS has read and will comply.**

The proposed ITS will allow an inmate to hear all call progress (i.e., ringing, busy, SIT, etc.) tones and messages when processing a call. The system will allow the inmate to hear the processing of the placed call to determine if a SIT with message or an answering device (i.e., answering machine, voice mail, etc.) has answered the call. The platform also provides very specific information to the inmate in the event a call is not completed. At no time will the system allow the inmate to speak (restricted voice channel) until the called party has positively accepted the call.

This is a result of the integration between SECURUS' validation system and the calling platform. Examples of the voice prompts provided to the inmates if a call was not completed are as follows:

- **"That number is restricted"**
- **"The number you have dialed has a collect call block"**
- **"Try your call again at a later time"**
- **"That is not a valid number"**
- **"This call is being terminated, dialing of additional digits is not allowed"**
- **"No calls are allowed at this time"**
- **"Your call was refused"**
- **"All circuits are busy"**
- **"No one is answering at this time"**
- **"No third party or credit card calls are allowed"**
- **"You have reached your maximum allowed number of calls" (PIN/debit).**

5.03.27 The proposed ITS shall not allow the inmate to speak to the collect-called party until the call has been accepted.

☑ **SECURUS has read and will comply.**

The proposed system requires positive 'called party' acceptance in order for two-way conversation to take place. When the called party answers the phone, the system's answer detection triggers the call acceptance voice message. This message announces the inmate's call and asks the called party if they wish to accept the charges of a collect call. The called party is instructed to dial a single digit on his or her own telephone instrument to accept the collect call charges, or hang-up to disconnect the call and refuse charges. The inmate cannot hear or speak to the called party until positive acceptance has occurred. This 'active' acceptance procedure ensures that the called party does not get billed for any charges that they have not authorized.

5.03.28 The proposed ITS shall allow the option for inmates to hear the processing of the placed call to determine if SIT tones with message or an answering device (i.e., answering machine and voice mail) has answered the call. Superintendents will determine whether or not this option will be used at their facility. At no time shall the ITS system allow the inmate to speak (restricted voice channel) until the called party has accepted the collect call.

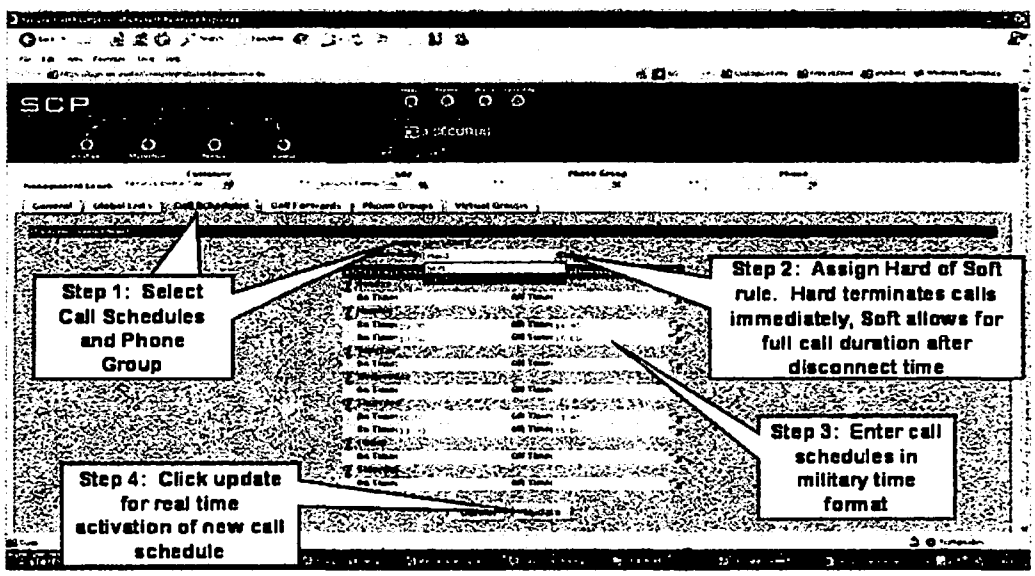
☑ **SECURUS has read and will comply.**

The proposed ITS will allow an inmate to hear all call progress (i.e., ringing, busy, SIT, etc.) tones and messages when processing a call. The system will allow the inmate to hear the processing of the placed call to determine if a SIT with message or an answering device (i.e., answering machine, voice mail, etc.) has answered the call. The platform also provides very specific information to the inmate in the event a call is not completed. At no time will the system allow the inmate to speak (restricted voice channel) until the called party has accepted the call.

5.03.29 The proposed ITS shall allow for DOC to program times when the system will be available or unavailable to inmate calling. The Offeror shall describe how this is accomplished.

☑ **SECURUS has read and will comply.**

Access for administration and investigation modules can be performed from any PC with access to the World Wide Web through a SSL secure website we call S-GATE. Users with the appropriate credentials login through S-GATE. Each level of administration are performed using "point and click" menus in S-GATE. Time availability can be assigned for multiple schedules per week or per day. Below is a typical screen shot of the S-GATE menu describing the four step process for assigning call times:



5.03.30 The Offeror shall supply the Security Threat Group (STG)/investigation Coordinator a system for operational information and electronic document management. This system shall provide an interface to the DOC offender tracking system, ITS call record database and other related systems. The Offeror shall provide all suitable software, hardware and network infrastructure to interface or link all DOC institutions, investigative offices and databases.

☑ **SECURUS has read and will comply.**

SECURUS offers the Alaska DOC multiple investigative solutions. All monitoring and administrative functions can be performed by authorized personnel remotely using the SECURUS provided Secure Gateway (S-GATE). S-GATE is a secure website allowing anywhere, anytime access via the World Wide Web. Authorized department personnel will be permitted access to the systems complete administrative capabilities from any internet equipped terminal regardless of its location. This internet access capability is in addition to direct access via provided monitoring terminals.

In addition, the system offers the Alaska DOC personnel and investigators the ability to access and review call record detail, commission information, and service request status online—anywhere and anytime through the Administrative Assistant Portal. This personalized portal provides a suite of expanded investigative tools for future implementation and use. This means the Alaska DOC will have the capability of constantly monitoring and auditing commissions and other critical data elements. The Alaska DOC will also have the ability to share information across the network, review commission statements, and access self-service reporting.

With the approval and cooperation of the Alaska DOC, SECURUS will provide integration to the Alaska DOC's existing Inmate Management System to help assist in the elimination of manual processes, such as PIN assignment and transfer, improve efficiencies in the Classification Department processes, and help facilitate an improvement to the timeframe in which inmates are able to contact friends and family members.

Scan Patrol is an exclusive SECURUS feature allowing an investigator to listen to a customizable number of seconds of a call in progress and then moves on to the next call, bypassing any inactive line. This feature enables an investigator to efficiently sample calls without the burden of manually selecting each individual call, thus allowing an investigator to perform other functions while monitoring the system. When the investigator hears something in a conversation that is of interest, he or she just clicks on the call in progress to move it into full time monitoring mode. Furthermore, facility personnel can forward a live call to an outside number for monitoring without alerting the inmate or called party.

Should the Alaska DOC be required to offer investigative services to outside agencies SECURUS' Electronic Dragnet is a suite of integrated web applications and services designed to help investigators and other law enforcement officials

efficiently analyze and process data such as criminal records, phone records, and visitation records.

5.03.31 The Call Processors shall have "hot swappable drives and power supplies.

☑ **SECURUS has read and will comply.**

The SECURUS Secure Call Platform has hot swappable Redundant Array of Independent Disk (RAID) drives and power supplies on each call processor. Additionally, our centralized system database is engineered with redundancy and disaster recovery planning to prevent loss of downtime and loss of data. All recorded conversations, call detail records and detainee profile information will be written twice to two separate Storage Area Networks (SAN) located in the centralized data center in Allen, Texas. In addition to the centralized storage redundancy, all data will then be replicated to the secondary data center in Dallas, Texas promoting disaster recovery in the unlikely event the Allen, Texas data center becomes inoperable.

Each data center is comprised of two fully redundant systems, each with its own circuit feed, its own physical racks, redundant communication, redundant termination carriers, and redundant A&B power with UPS and generator backup. The physical storage itself is also advanced; the data is stored via both SAN and archives are performed by robotic tape, and the data centers are connected to one another by an Optical Carrier Network Ring. This system features full state awareness with the ability to fail over to the backup data center if necessary without dropping the call in progress or loss of data retention.

5.03.32 The Offeror is required to provide the line voltage outlets for all equipment.

☑ **SECURUS has read and will comply.**

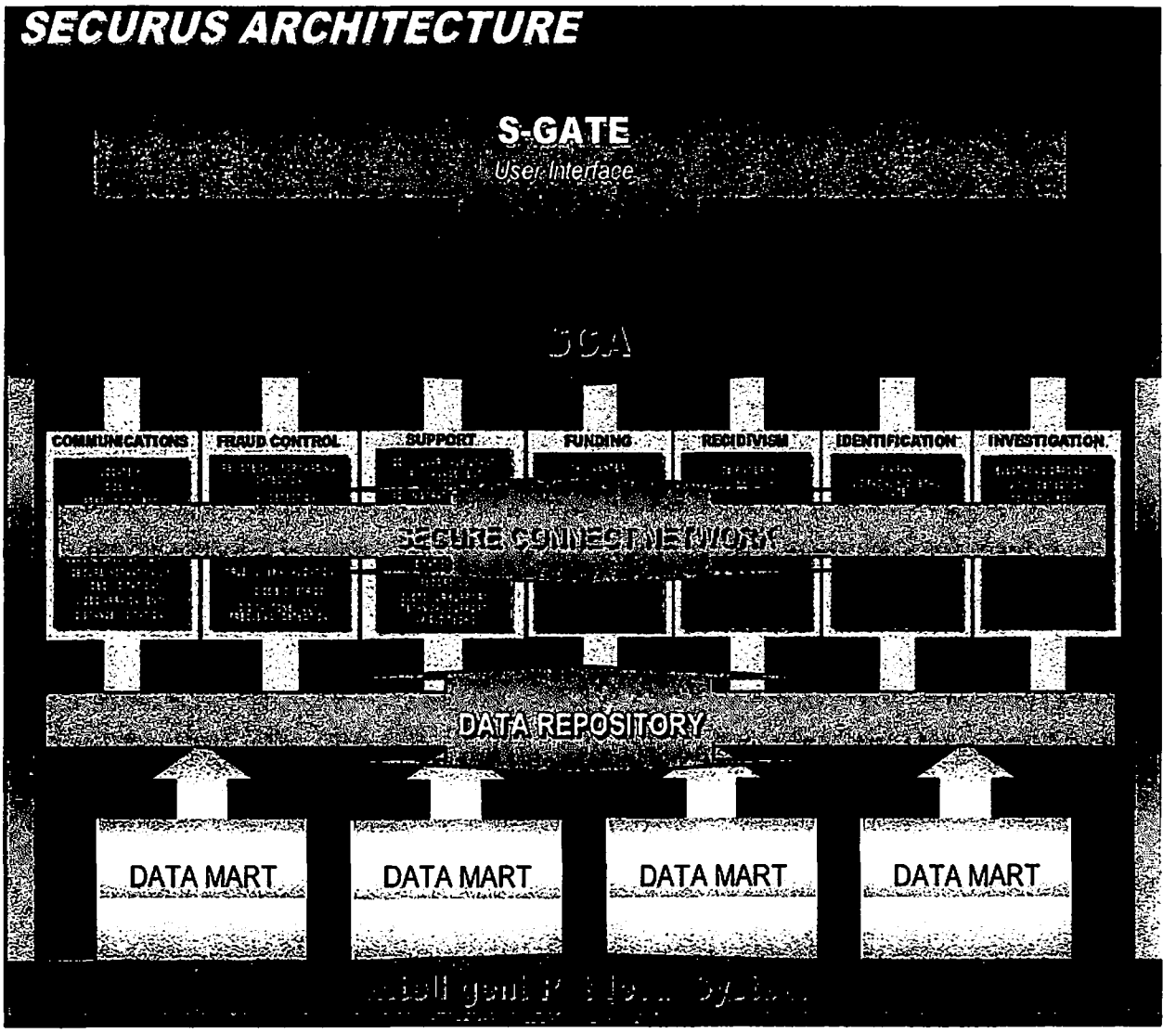
5.04
Central Database

5.04.1 A network and central database shall be provided and managed by the Offeror at no cost to the DOC. The purpose of the database is to provide full database redundancy for all Call Processors at each DOC facility and to provide pooled data for investigators analysis. The Proposal shall describe the details of the proposed network.

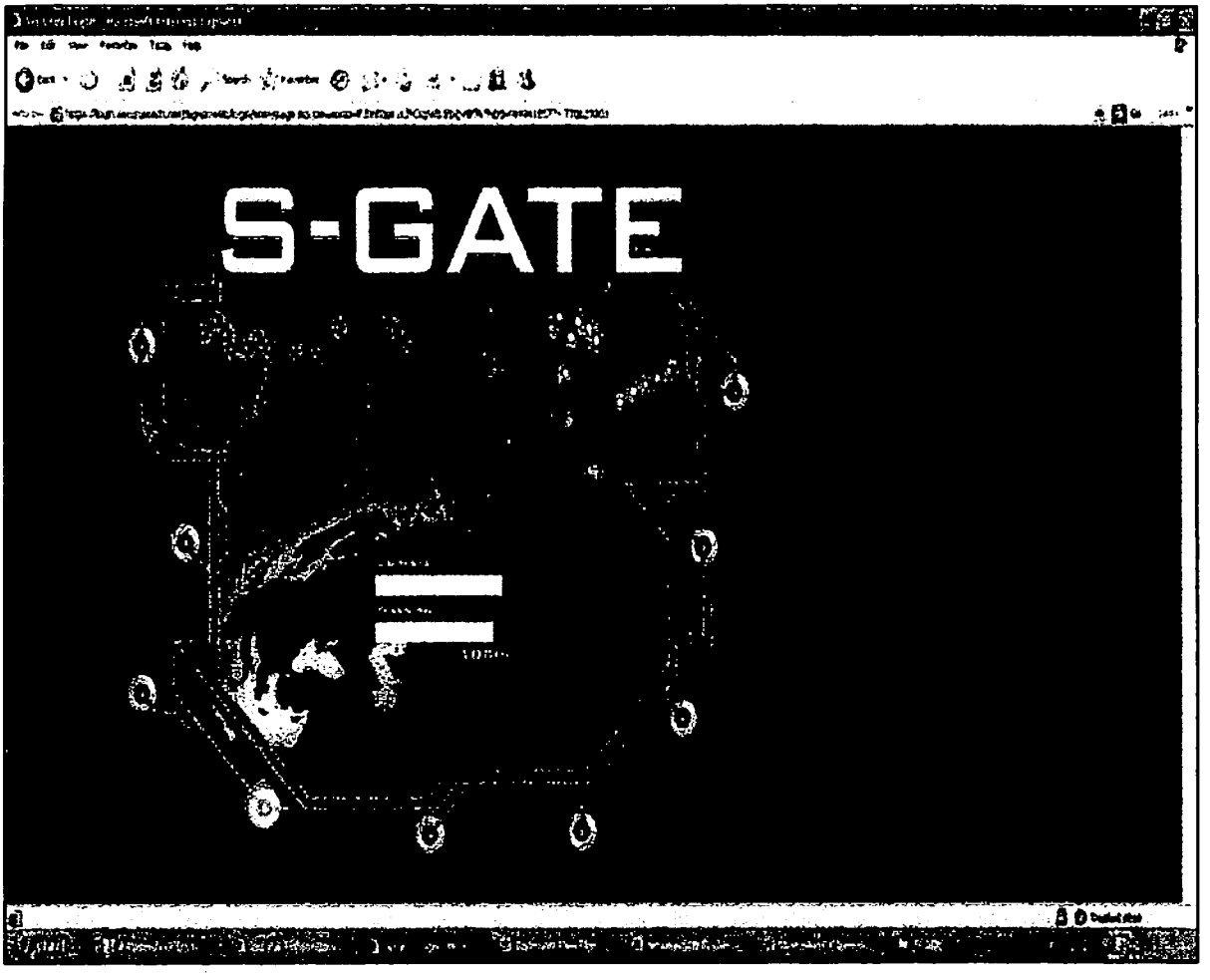
☑ **SECURUS has read and will comply.**

Secure Connect Architecture (SCA) along with the S-Gate, a single entry web portal Graphic User Interface (GUI) for correctional facilities and friends and families of the inmates is additional evidence of our commitment and investment to meet the needs of the correctional industry.

Secure Connect Architecture and S-Gate provide the foundation of a future array of software applications that will include video, voice, data, biometric and other capabilities.



SECURUS' S-Gate Portal opens a secure window into a facility's operations providing authorized personnel with the access to an array of applications, functions and modules that are design to aid correctional facilities in maintaining safe and efficient operations. Whether you investigate inmates' potentially fraudulent activities, require technical support, available 24 hours a day, 365 days a year.



The infrastructure supporting the Secure Call Platform (SCP) was designed and built with 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.

Massively Distributed Client/Server Architecture
SECURUS' Secure Call Platform™ call management system runs on our SCN - Secure Connect Network™, one of the only net centric, VoIP, digital transmitted systems in the industry. This assures that all Secure Call Platform calls utilize a digitally "clean" transmission flow.

The Secure Connect Network (SCN) "Clean Line" Difference
"Clean" digital transmission is not only a more efficient means of transport, assuring more calls are completed and operational efficiencies achieved. It also increases the effectiveness of investigative and fraud tracking programs such as 3-Way call detection, word search applications and voice biometric identification systems. Additionally, these "clean" transmissions result in better call clarity for end users, decreasing complaints from the community.

Complete Flexibility
Secure Call Platform's enhanced capabilities allow facility personnel complete control over most system features. User friendly functionality allows facility staff to turn on a pod, restrict a phone, change a language, or turn on or off a feature or application. All this and more can be easily accomplished with the click of a button. Your system will have the flexibility to conform to all of your facilities operations and requirements, not requiring you to conform to an inflexible system.

Immediate Upgrades
The system also allows for immediate system-wide upgrades and repairs from one central location, eliminating the need to wait for a field technician to access your system on-site. The ease of upgrading your system enables us to assure the Alaska DOC that they will always be equipped with the latest technology and never utilize an obsolete system.

Data Security
Facilities no longer have to fear losing data because of local disasters such as hurricanes, floods, fires, localized security breaches or lightning. All facility data is replicated on regionalized, fully redundant data repositories for easy secured retrieval, from any location, by any DC authorized users only. If there is an MPLS outage or a call processing outage, the user will still have access to calling data for inquiry and investigation purposes. Access issues and loss of data due to hard drive or other system failures are a thing of the past. The platform's fully redundant system is placed in a Class IV Disaster Resistant Data Center to assure data integrity.

Pro-Active Flexibility
Secure Call Platform allows SECURUS personnel to remotely monitor not only hardware issues but also to pro-actively monitor call flow activity, data transmissions and specific phone activity, to assure your system is running at peak performance.

Inmate Calling Service Reliability
Reliability is not just a word for us. No technological achievements will serve the customers well if applications fail to meet high reliability standards that our customers expect from us. We strive to address every aspect of ITS that affects reliability. That starts with stringent component procurement processes and finishes with built in operational redundancy, data centers disaster recovery, network protection, power backup and many more aspects.

In support of our customers, SECURUS operates and maintains three major data centers. The core network topology has a redundant Optical-Ethernet-Ring connecting all three locations together. Each data center has it own Internet connection, UPS, and generator to insure maximum facility uptime. The traditional data circuits (MPLS, Frame Relay, and VoIP) all have dual connectivity feeds to and from the Telecommunication Carrier to our data centers.

SECURUS has invested heavily to create a very reliable high availability IT infrastructure. All major IT equipment (Routers, Switches, Firewalls, Servers, SAN, etc) both internal and external (customer facing) have built-in hardware redundancy. Business applications that are classified as mission critical are supported by a Disaster Recovery Solution based on a mutually beneficial service level agreement. SECURUS' centralized data center is in Allen, Texas, with a secondary data center in Dallas, Texas and a Disaster Recovery data centers in Irving, Texas. These data centers provide SECURUS with both site-level and server-level redundancy. SECURUS recently completed the process of building a regional data center to support the Secure Call Platform infrastructure in Atlanta, Georgia. Additional sites are being reviewed if the need arises.

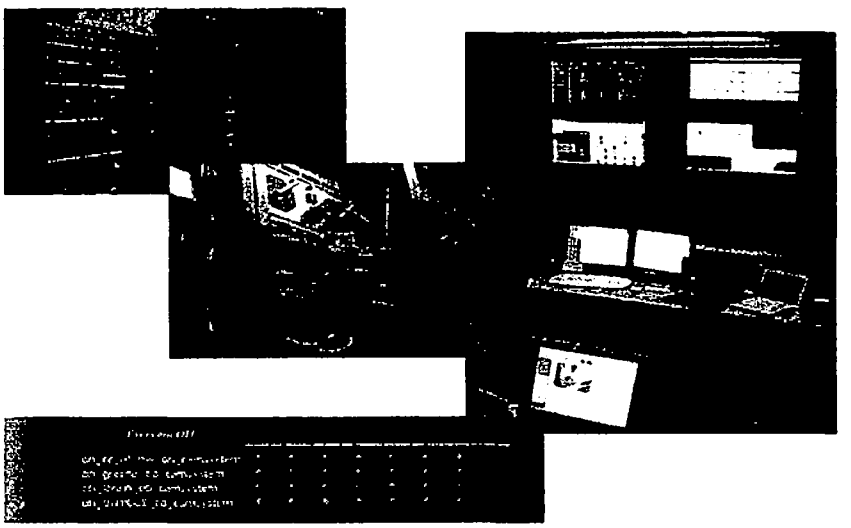
Network Protection

SECURUS applies a high level of security to protect our customers and ourselves from cyber-pirates. Applications transmitting data across public networks are supporting SSL, CERTS, and 128 bit encryption. Cisco and Juniper firewalls are utilized throughout the network to protect SECURUS and its customers by creating DMZ networks, which result in multiple levels of firewall protection. In addition, Tipping-Point Intrusion Prevention System (ITS) and Intrusion Detection Systems (IDS) devices are used at our data centers and at the corporate headquarters. All Servers, laptops, workstations require anti-virus & anti-spyware protection software and latest operating systems patches. SECURUS supports both AVG and Symantec anti-virus.

Network and Site Monitoring

The SECURUS network consist of many servers each providing a different business critical application or service. All applications that affect the business are monitored.

SECURUS proactively identifies potential system and network abnormalities through our centralized suite of diagnostic applications



Allen, Texas Data Center
SECURUS' centralized data center in Allen, Texas, is a Class IV data center (the highest non-military classification).

5.04.2 The new network shall be compatible with the existing DOC networks (i.e., TCP/IP) and capable of network speeds equivalent to the DSL or faster.

☑ **SECURUS has read and will comply.**

5.04.3 The Centralized Database shall be located at an Offeror-provided site, located outside of DOC facilities. The Proposal shall describe the facilities and location of the Centralized Database.

☑ **SECURUS has read and will comply.**

SECURUS' has a centralized data center in Allen, Texas, a secondary data center in Dallas, Texas and a Disaster Recovery data center in Irving, Texas. These three data centers provide SECURUS with both site-level and server-level redundancy. SECURUS recently completed the process of building a regional data center to support the Secure Call Platform infrastructure in Atlanta, Georgia. Additional sites are being reviewed if the need arises.

Each remote site can be connected to a central site using SECURUS-provided bandwidth. This connectivity provides a data link from the remote platforms to the central site for transferring call records and user profiles. Call records are generated centrally and reports and data can be retrieved from remote sites.

New or updated user profiles and system configuration data are managed centrally through the Secure Call Platform and can be updated by authorized users at any site. Authorized users from any sites have the ability to login to operate the system, change system configuration, troubleshoot, and retrieve data. The system security features at both the central site and each remote site strictly control this operation. System operators must have a security clearance based on passwords, user –IDs, and security levels to gain access to any individual features of the proposed ITS.

Component Redundancy
With the SECURUS system, the chance of total system failure is essentially eliminated because in the event that any one component fails, the system will automatically switch to another, properly functioning component – in most cases with no disruption to service. The system enhancements that allow for such comprehensive reliability are listed below:

- Every 24 phones or less get own IAD
- Phones diverse wired with multiple IAD
- Each IAD has diverse T1s
- T1s use MPLS to primary & backup data centers
- Unique wiring scheme with separate hardware
- Centralized system using carrier class components to minimize downtime
- Use of public internet connection for connectivity in case of failure in point-to-point connection

Data Back-ups and Storage
The redundancy built in to the SECURUS system effectively prevent loss of data and system downtime because all of the data is stored in an offsite, centralized database and backed up at multiple locations across the nation. Because the system is web-based, the data can be accessed at any location with an internet connection, and SECURUS' Secure Connect Architecture maintains the system at the highest level of operability.

In addition, all call records will be duplicated and backed-up at the fully-staffed data centers in Allen and Dallas, Texas. Each data center comprises two fully redundant systems, each with its own circuit feed, its own physical racks, redundant communication, redundant termination carriers, and redundant A&B power with UPS and generator backup. The physical storage itself is also advanced; the data is stored via both SAN and robotic tape, and the data centers are connected to one another by a Metropolitan Area Network Ring. Additionally, the system features full state awareness of each call with the ability to fail over to another data center if necessary, in most cases without dropping the call in progress.

5.04.4 The Centralized Database shall be in Oracle TM or MS SQL 78 or other open architecture software. The Proposal shall describe Central Database details.

☑ **SECURUS has read and will comply.**

All of the SECURUS system's functionality is based on the Oracle multi-user relational database management system, which provides powerful tools for the creation, maintenance, and administration of large databases. Oracle gives the system the ability to organize and process large amounts of data in a fast and efficient manner. Oracle has significant data replication capabilities that provide substantial data backup security.

The proposed ITS stores all call information in non-volatile memory located within the system. This data is kept in a proprietary format that provides detail for management reports, fraud analysis, and conversion to industry standard billing formats. The platform is capable of storing multiple months of records at the site; however, all Call Detail Records are collected daily in SECURUS' data center for billing purposes and are archived at the secure data center.

5.04.5 The Proposal shall describe how it will provide ITS system security for all data stored in the local and central databases. Such a security description must include system security, including levels of encryption, as well as how access to such sensitive information will be performed within the Offeror's organization.

☑ **SECURUS has read and will comply.**

Data Security
Facilities no longer have to fear losing data because of local disasters such as hurricanes, floods, fires, localized security breaches or lightning. All facility data is replicated on regionalized, fully redundant data repositories for easy secured retrieval, from any location, by any Alaska DOC authorized user's only. If there is an MPLS outage or a call processing outage, the user will still have access to calling data for inquiry and investigation purposes. Access issues and loss of data due to hard drive or other system failures, are a thing of the past. The platform's fully redundant system is placed in a Class IV disaster resistant data center to assure data integrity.

Pro-Active Flexibility
Secure Call Platform allows SECURUS personnel to remotely monitor not only hardware issues but also to pro-actively monitor call flow activity, data transmissions and specific phone activity, to assure your system is running at peak performance.

Network Protection
SECURUS applies a high level of security to protect our customers and ourselves from cyber-pirates. Applications transmitting data across public networks are supporting SSL, CERTS, and 128 bit encryption. Cisco and Juniper firewalls are utilized throughout the network to protect SECURUS and its

customers by creating DMZ networks, which result in multiple levels of firewall protection. In addition, Tipping-Point Intrusion Prevention System (IPS) and Intrusion Detection Systems (IDS) devices are used at our data centers and at the corporate headquarters. All Servers, laptops, workstations require anti-virus & anti-spyware protection software and latest operating systems patches. SECURUS supports both AVG and Symantec anti-virus.

Network and Site Monitoring
The SECURUS network consist of many servers each providing a different business critical application or service. All applications that affect the business are monitored.

Facility Monitoring
Redundant monitoring systems, all with paging capability, are in place, alerting on-site engineers of any system threshold inconsistencies. Redundant page alerts are also sent to the Network Operations Center (NOC) to create a Ticket of the event, which is then sent to the data center via e-mail, page, and phone call, as a redundant notification process.

The onsite infrastructure engineers make scheduled daily inspections of all infrastructure systems and routinely perform preventative maintenance.

Security
The SECURUS centralized data center in Allen, Texas, with a failover redundant site in Dallas, Texas, maintains some of the most comprehensive security measures in the industry. Access to network facilities is controlled through six levels of mandatory physical security and an escort is required in areas that house critical components of our system.

5.04.6 The DOC shall be able to perform queries and request reports from the Centralized Database. The Proposal shall describe the availability of the report writer for this use.

☑ **SECURUS has read and will comply.**

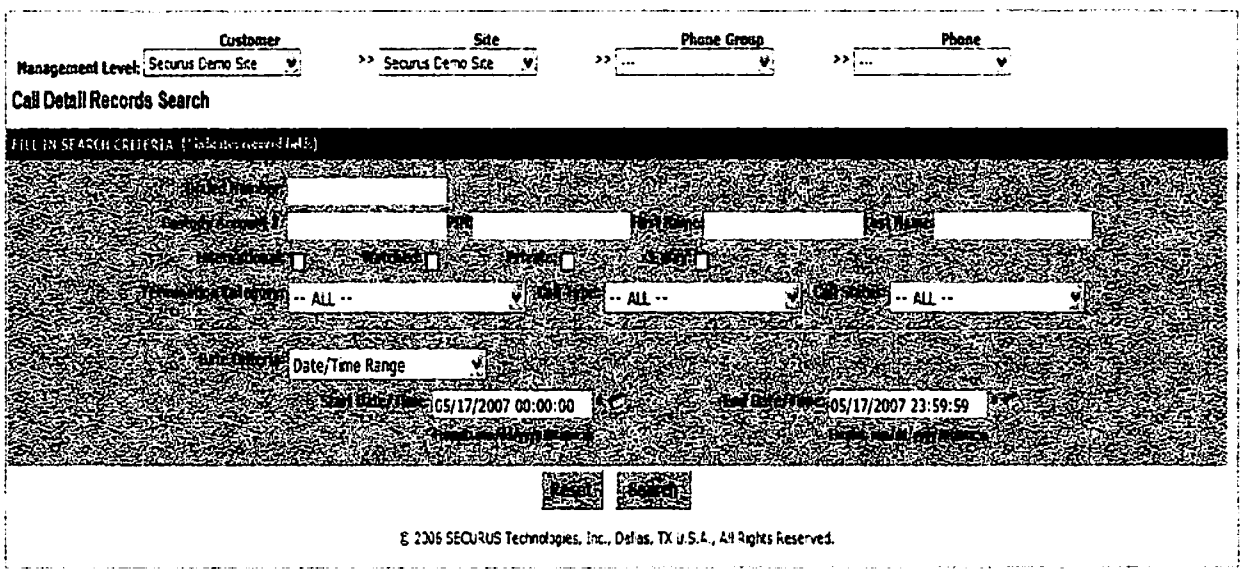
The Secure Call Platform has a dedicated reports writer that provides investigative information based on the Call Detail Records. This sophisticated reporting tool can provide routine scheduled reports, or reports on an ad hoc basis. This means, in almost every case, the Alaska DOC will be able to create your own reports, selecting whichever criteria you need included. These reports are available immediately.

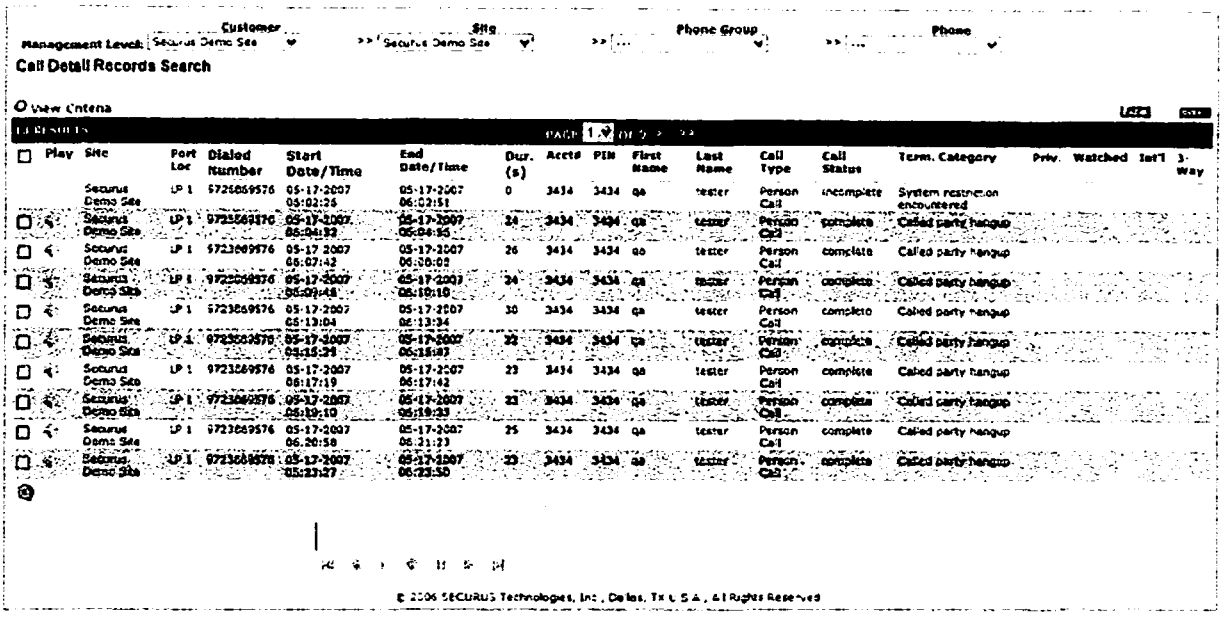
The Secure Call Platform is capable of searches and call detail analysis on all calls placed from each inmate telephone through the system which includes date, time and duration, telephone number or origination and destination, if utilized, inmate ID, reason for termination, and much more. Call details are kept on all call attempts, except those to blocked numbers. The standard reports can be customized by varying search criteria such as date range, facility, or call length.

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

- **Per phone, per location and per inmate**
- **Destination number (partial and/or full number entry)**
- **Date and time range**
- **Call duration and call frequency**
- **Call type (i.e. completed, incomplete, blocked, etc.)**
- **Number restriction and/or status assignment**
- **Personal allowed number cross-referencing**
- **Graphical display of call fluctuation**
- **Local, intralata, interlata, interstate and international**
- **Broad search with no data entry**
- **Suspected fraudulent call activity**

Call detail search parameters and a sample report are shown below.





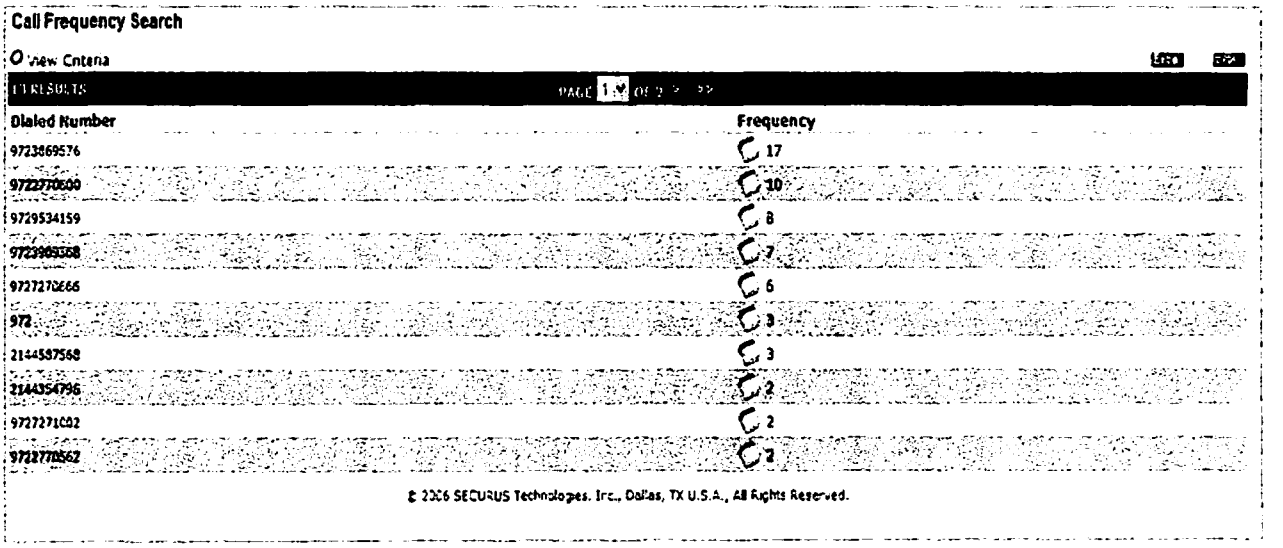
Investigative Reports

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 no limits to the type of information available through Investigative Reports. This unique application will even assist you in generating a report with little or no concrete information available. For example, our Frequently Called Number Report (FCN) will display information relative to the amount of calls to a particular number and reflect the location(s) from within the facility the number was called.

The FCN feature allows investigators to generate a report by entering a frequency threshold that instructs the system to search for only those numbers that have been called 'x' amount of times throughout the facility. For example, by entering '50' in the parameter field the system will display only those numbers that have been called 50 or more times within a designated timeframe. Once the report is displayed on screen a simple click of the mouse will automatically produce a second report that represents all areas of the facility from which a specific number has been called. From this report investigators can analyze data to determine specific call patterns, detail suspicious activity and selectively assign a watched number status to potential fraudulent numbers.

A sample *Frequently Called Number Report* is shown below.

PROPRIETARY AND CONFIDENTIAL



Web Portal

The SECURUS Web Portal will provide the Alaska DOC with the ability to access, share and review call record detail, commission information, and service request status online—anywhere and anytime. This means the Alaska DOC will have the capability to continuously monitor and audit commissions and other significant data elements.

SECURUS' Portal opens a secure window into a facility's operations, providing authorized personnel with the access to an array of applications, functions and modules that are design to aid correctional facilities in maintaining safe and efficient operations. Whether you need to investigate inmates' potentially fraudulent activities or require technical support, all functions are available 24 hours a day, 365 days a year.

5.05
Personal identification Numbers (PINS)

5.05.1 The ITS shall restrict use through authorized Personal Identification Numbers (PINs) assigned to each inmate. The length of these PINs shall be determined by DOC and remain consistent throughout DOC facilities.

☑ **SECURUS has read and will comply.**

5.05.2 The ITS shall use DOC's inmate PIN assignments and numbering plan and have provisions for assigning PINS through a random automatic method. Current PINS are numeric only and may be up to fifteen (15) digits long. PINS are permanently assigned.

☑ **SECURUS has read and will comply.**

With SECURUS' system, each inmate is assigned a unique Personal Identification Number (PIN), ranging anywhere from four (4) to sixteen (16) digits. This range creates a maximum number of nine (9) billion PIN combinations. The system has the ability to randomly generate PINs and automatically assign PINs to the inmate.

5.05.3 The ITS shall be capable of de-activating the PIN feature by individual inmate telephone, groups of telephones and/or entire institutions, at DOC's option. At no time shall the inmate telephones be unrestricted due to the deactivation of the PIN feature. **The PIN system should provide for voice activation/verification.**

☑ **SECURUS has read and will comply.**

De-activating PIN Feature
A single inmate's PIN or any number of inmates' PINs may be suspended for a specified period of time from either the on-site Administrative terminal or an authorized remote terminal. This Suspension feature is frequently used for punitive reasons and allows the facility to deny telephone privileges to one or more inmates without affecting other inmates sharing the same inmate telephones. The length of time for PIN denial is input and automatically policed, enforced, and released by the system. The system will automatically reset the PIN to allow calls on the day requested so no manual intervention is needed. This feature allows inmates, if necessary, to still make privileged calls even while being suspended from other calls. Direct manual control of this suspension feature is also allowed from the on-site administrative terminal or authorized remote terminal.

Voice Biometrics Inmate Identification Service (Optional)
The Voice Biometrics system has been deployed for over eight years in local, county, and state correctional institutions and is successfully verifying the identities of over 50,000 Inmates a day. Voice Biometrics is the only inmate voice biometric identification service successfully deployed in correctional facilities. The system works with existing inmate telephones and introduces no expensive new hardware into secure areas where inmates can tamper with it. Voice Biometrics technology is a proactive security system; it works without human involvement, eliminating the need for staff to monitor screens, listen to phone calls, or maintain biometric equipment in secure areas when it is damaged by the inmates.

Voice biometrics makes it practical for all correctional facilities to assign PIN numbers to inmates. Currently, in high turnover institutions the cost and effort required to administer PIN "calling lists" for all inmates is often too great. In facilities that do have "calling lists", the ability to eliminate those lists will have a positive impact on the number of calls from the facility which will increase the revenue to that facility. Since the system will identify the caller, the facility can trace all calls made from an inmate or specific telephone. This will allow the

facility to investigate those individuals making fraudulent or harassing calls, and eliminating the need for "calling lists".

When an inmate is booked into a facility, he/she will enroll by being asked to say his/her name into a preprogrammed phone, four times. This process takes one minute or less. These repeated utterances of his/her name become the basis for the inmate's personal voice signature. When an inmate wishes to place a call from within the facility, they must first key in a PIN. These PIN numbers can be setup to auto generate from the Secure Call Platform. The system will prompt the inmate to say their name. Once approved, which takes less than a second, the inmate can continue to place the call. If the verification is not approved, the inmate will receive a message stating that the voice was not verified and the call will end, forcing the inmate to start a new, fully-controlled call.

Voice Biometrics Administrative Tools will allow officers the ability to search and listen to each caller's voice utterance. Investigators will have the tools needed to trace those inmates willfully trying to commit fraud or harassment from within the facility.

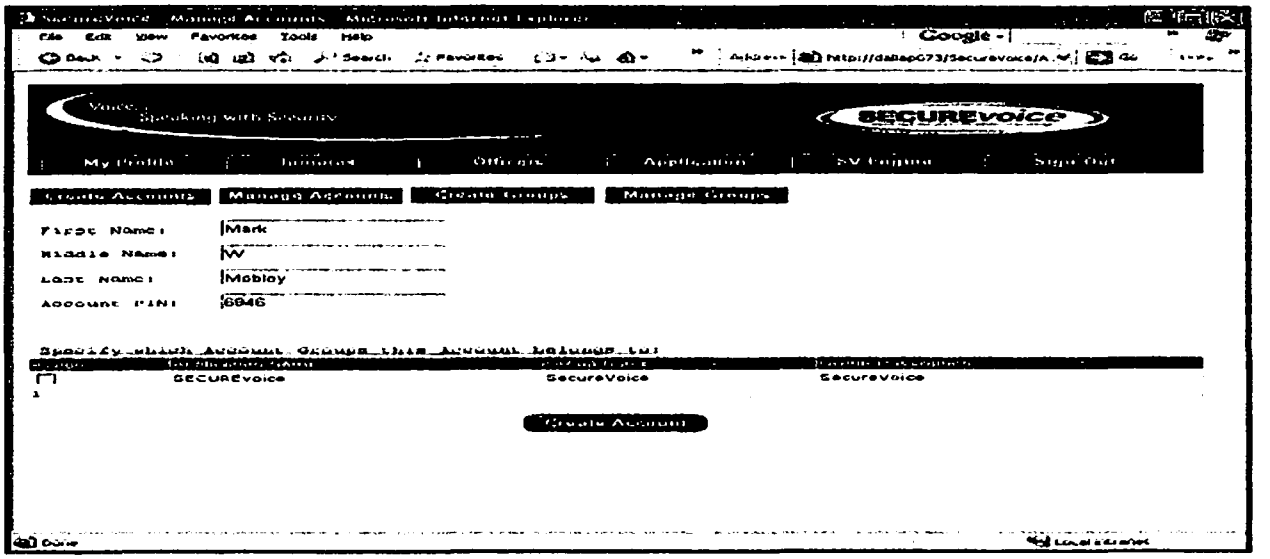


Figure: SECUREvoice™ includes a user-friendly, easy to use interface.

With Voice Biometrics, the call is linked to the inmate placing the call by both the voice response and the personal identification number. SECURUS is experiencing very high rates of accuracy with this product. The primary administrative tasks will be performed during the enrollment process. Each inmate will record his or her name three times, and PIN numbers will be assigned. After the enrollment, there is very little administration required.

The scientific principle behind Voice Biometrics is the fact that every person's voice creates a unique signature. Voice Biometrics accurately captures a voice print, stores it, and later compares it to a person's voice to validate their

identity. A voice print cannot be imitated. SECURUS has benchmarked our speaker verification technology on a telephony database having 11,224 trials and our system performed at 98.9% accuracy. Here, less than 1.1% of the true users were denied and less than 1.1% of imposters were accepted. This performance was measured for the worst-case scenario where the imposter knew the password of the person being impersonated. In the case where the imposter does not know the password of the user that he or she is trying to impersonate, the accuracy would be well above 99%.

5.05.4 The ITS shall allow each PIN to have a "class of service" assigned (i.e., duration of each call). The proposed ITS system shall provide call restrictions by PIN that provide all of the following restrictions:

A. Inmates can be either approved or not approved to make phone calls by PIN.

☑ **SECURUS has read and will comply.**

B. Inmates, via the PIN, can be restricted to a specific telephone or group of telephones, at DOC's option.

☑ **SECURUS has read and will comply.**

C. Limit duration of call. Maximum call duration can be set globally (all PINs), by site, by facility area or by individual inmate's PIN, at DOC's option and can be set for each type of call (Local, intraLATA, interLATA, interstate).

☑ **SECURUS has read and will comply.**

With SECURUS' calling platform, inmate call duration is completely programmable by call type and may be limited to a specific time. A default time limit is provided for the entire system and individual groups can be added for specific telephones as well as inmates within a group. The time limit may be changed for each active phone, individual inmates, and/or the entire system. Additionally, the Alaska DOC can choose to limit the number of calls per day or week, hours during which calls can be made, and the type of calls that can be made during each time period.

D. Restrict time of day calling. An allowed calling schedule can be provided for each specific PIN, by facility area, by site and globally (all PINs). The global restrictions can take precedence over individual PIN restrictions, at DOC's option.

☑ **SECURUS has read and will comply.**

The Secure Call Platform permits the automatic, regular, immediate cut-off of all inmate telephones at once, groups of telephones (e.g. an entire building or wing), or individual telephones, and the ability to pre-select hours of operation by telephone or group of telephones.

The Secure Call Platform allows for unlimited time-based control of inmate calling. As with most features, calling times can be configured on a per minute, per phone, per group, per facility, or system wide basis. Multiple allowed/ prohibit call times can be configured each day of the week. For example, one area can be configured to come on at 8:00 AM, go off at 12:00 PM, come back on at 2:00 PM and go off again at 10:30 PM, while another area can be configured to come on at 10 AM, and go off at 11:45 PM.

E. Limit calling privileges. Restrict an inmate under disciplinary action from placing calls. The Proposal shall describe how these restrictions can be accomplished.

☑ **SECURUS has read and will comply.**

A single inmate's PIN or any number of inmates' PINs may be suspended for a specified period of time from either the on-site Administrative terminal or an authorized remote terminal. This suspension feature is frequently used for punitive reasons and allows the facility to deny telephone privileges to one or more inmates without affecting other inmates sharing the same inmate telephones. The length of time for PIN denial is input and automatically policed, enforced, and released by the system. The system will automatically reset the PIN to allow calls on the day requested so no manual intervention is needed. This feature allows inmates, if necessary, to still make privileged calls even while being suspended from other calls. Direct manual control of this suspension feature is also allowed from the on-site administrative terminal or authorized remote terminal.

5.05.5 The ITS shall have the ability to limit calls to a specific duration by PIN and by specific telephone numbers assigned to a PIN.

☑ **SECURUS has read and will comply.**

The Secure Call Platform provides an approved inmate specific pre-determined calling list (Personal Allowed Numbers: PAN) with a specific number of telephone numbers for each PIN. The lists in the SECURUS system will be capable of differentiating between social callers and attorneys. In the system's standard configuration, each inmate is allowed to register from one (1) to twenty (20) telephone numbers. The facility will determine the maximum number of telephone numbers each inmate is allowed to register. Registration of a telephone number includes the number, name of the party who the inmate wishes to call, and the relationship of that party to the inmate.

The PAN Editor provides options to mark a selected PAN entry as Free, Blocked, Private, or Watched and includes a Line Information Data Base (LIDB) option which automatically validates the PAN entry number associated with the selected inmates PIN number to verify that the phone number is a valid number.

The telephone numbers registered by each inmate are identified with the inmate's PIN and are resident in the system.

5.05.6 The ITS PIN feature shall ensure that the automated operator function uses the inmate's pre-recorded name (recorded in either the inmate's voice and language, or in the voice of an administrator) to announce to the called party from whom the call is originating. Identification of the specific inmate and thus the announcement of the inmate's name shall be performed by the PIN assignment.

☑ **SECURUS has read and will comply.**

The automated operator function uses the inmate's pre-recorded name (recorded either in the inmate's voice and language, or in the voice of an administrator) to announce to the called party from whom the call is originating.

5.05.7 The Offeror shall use an announcement similar to the existing announcement. This announcement shall be subject to DOC approval and include rate information.

☑ **SECURUS has read and will comply.**

Upon receiving a call from an inmate, the called party will hear an announcement similar to the following:

> ***"Hello, you have a collect call from (INMATE NAME), an inmate from an Alaska Correctional Facility. To accept charges press zero (0); to refuse charges press one (1) or hang up now; to block your number from receiving future calls from this facility, press six (6); to obtain a rate quote press four (4). If you use three way calling or call waiting, you will be disconnected. All call detail and conversations excluding approved attorney calls, will be recorded."*** **After acceptance of call, "This call is subject to monitoring and recording. Thank you for using SECURUS".**

5.05.8 The Proposal shall explain, in detail, the entire process of PIN administration including, without limitation, the maximum number of digits and the procedures and methods of assigning or changing PINs.

☑ **SECURUS has read and will comply.**

Prior to system implementation, SECURUS would propose an integration with your current offender management system for a bi-directional feed on inmate intakes and releases. This automated feed will reduce staff time requirements for the use of this important administrative feature. The Alaska DOC may dictate what numerical identifiers will be used for each inmate PIN.

In order to replicate of inmate profile information located in the existing Personal Identification Numbers (PIN) and Personal Allowed Numbers (PAN) database, as the current provider SECURUS recommends transferring this data from the existing inmate telephone system in an importable file format.

SECURUS will work closely with the Alaska DOC to insure accurate and timely information is imported immediately prior to final cutover at each institution. The process will require data entry of new residents at each facility to be held while file conversion, testing of data integrity and deployment takes place. Once the new database and telephone service is restored, new resident profile information will be entered directly into the new SECURUS system.

The Inmate Telephone Service (ITS) can be Personal Identification Number (PIN) driven. The ITS will restrict use of the service through authorized PINs assigned to each inmate. No PINs will be issued by any institution. This PIN service will allow individual PINs to be shut-off upon request of staff at the facility. When an inmate transfers to a different institution, that inmate's PIN account will also be transferred.

Each inmate is assigned a unique PIN, using the Alaska DOC's coding, an automated feed through the inmate management system or a system assigned PIN. The PIN can be as many as 16 digits. When the handset is removed from its cradle, the inmate telephone provides audible instructions prompting the inmate to dial his or her PIN.

The SECURUS ITS PIN database includes first and last name entries enabling cross reference searches by name. A screen similar to the one shown below is displayed with name and the additional fields that are available in the PIN database.

Administration of all inmate PINs will be limited as required by the Alaska DOC. The PIN system is enabled as a Port Class of Service option within the Automated Operator Service and can be applied to a single phone, group of phones, or all phones in a facility. The PIN system can be configured to operate in one of three (3) primary modes. Each mode is progressively more restrictive.

The system can be set to make a phone call either by PIN or without the use of PIN. Inmates, via the PIN can be restricted to a specific telephone or group of telephones, at the Alaska DOC's option. The Department can set maximum call duration globally (all PINs), by site, by facility area, by individual inmate's PIN, or by type of call (Local, IntraLATA, InterLATA).

Through the proposed ITS, the Alaska DOC can institute an allowed calling schedule for each specific PIN, by facility area, by site and globally (all PINs). The global restrictions can take precedence over individual PIN restrictions. The Department can restrict an inmate under disciplinary action from placing all calls assigned to their particular PIN with the exception of privileged numbers (e.g., attorney, approved clergy and social work professionals). The Department can set call duration, set number of calls per day, set only certain numbers per PIN, etc.

The SECURUS PIN feature ensures that the automated operator function uses the inmate's pre-recorded name (recorded in either the inmate's voice, or in the

voice of an administrator) to announce the called party from whom the call is originating.

The SECURUS ITS allows the recording of inmate calls to be discontinued when certain pre-determined telephone numbers (privileged telephone numbers) are called. The proposed ITS will provide for telephone lists to be assigned to each particular inmate's account information. These telephone lists will be restricted and controlled by the inmate's PIN.

Below are the three primary modes, which may be applied to a single phone or group of phones in a facility:

Mode 1 – Open PIN: This is the most basic mode of operation and the simplest to administer. Each inmate is assigned a unique PIN that will be required to make a phone call; however, no individual phone number restrictions or calling lists are utilized in this mode. Only global system calling restrictions will be applied to the inmate's calls.

Mode 2 – Open PIN with Restrictions: Mode 2 builds on the Mode 1 Open PIN feature and adds the ability to place restrictions and limits on specific phone numbers, while allowing all other phone numbers to be processed as they would in an Open PIN system. Mode 2 restrictions can also include the recording and alarming of numbers, language options, special parameters for destination numbers, and the use of facility or global number lists.

Mode 3 – Closed PIN: Mode 3 provides the most restrictive type of calling privileges; however, it is also the most administration-intensive of the three modes. In the system's standard configuration, each inmate is allowed to register from one (1) to thirty (30) telephone numbers he or she wishes to call, up to a total of 150,000 individual 11-digit numbers. The total number of destination numbers available to put on an inmate's list is unlimited. The facility will determine the maximum number of telephone numbers each inmate is allowed to register. Registration of a telephone number includes the number, name of the party who the inmate wishes to call, and the relationship of that party to the inmate. The telephone numbers registered by each inmate are identified with the inmate's PIN and are resident in the system. Only that specific PIN may validate calls to those numbers. Updating calling lists is a continuous process as inmates are booked into, or released from the facility, or as the inmates request changes to their calling lists. This type of control is usually recommended only for facilities with a low rate of inmate population turnover or where such extreme security measures are deemed desirable. Note that in a Closed PIN environment, the facility may choose to make certain telephone numbers "commonly available" to all inmates. There common numbers may be assigned Global and/or Facility Accounts.

The proposed ITS will allow for telephone numbers to be assigned to each particular inmate's account information. These telephone numbers will be placed in the particular inmate's "Approved Number List" assigned to the

inmate's PIN. The total number of destination numbers available to be put on an inmate's list is currently 1,000, but even this number can be increased at the direction of the Alaska DOC. Therefore, the maximum amount of telephone numbers available for inmates to call is at the complete discretion of each facility within the Alaska DOC.

A single inmate's PIN or any number of inmates' PINs may be suspended for a specified period from either the on-site Administrative terminal or an authorized remote terminal. This Suspension feature is frequently used for punitive reasons and allows the facility to deny telephone privileges to one or more inmates without affecting other inmates sharing the same inmate telephones. The length of time for PIN denial is input and automatically policed, enforced, and released by the ITS.

The length of time for PIN denial is input and automatically policed, enforced, and released by the ITS. The proposed ITS will automatically reset the PIN to allow calls on the day requested so no manual intervention is needed. This feature allows inmates, if necessary, to still make privileged calls even while being suspended from other calls. Direct manual control of this suspension feature is also allowed from the on-site administrative terminal or authorized remote terminal.

5.05.9 The DOC may integrate the ITS with a management system for the automatic assignment of PINs. The Proposal shall describe how this will be accomplished.

☑ **SECURUS has read and will comply.**

SECURUS can provide an interface with the Alaska DOC's offender management system, which will provide for the facility to choose a number from the offender management system to be used as the PIN for the inmate phone system. This number and inmate number will automatically be entered into the phone system upon the inmate being booked into the facility.

5.05.10 The ITS shall allow for a restricted number list of telephone numbers to be linked to an individual PIN. DOC personnel shall enter such telephone number lists.

☑ **SECURUS has read and will comply.**

The Secure Call Platform provides an approved inmate specific pre-determined calling list (Personal Allowed Numbers: PAN) with a specific number of telephone numbers for each PIN. The lists in the SECURUS system will be capable of differentiating between social callers and attorneys. In the system's standard configuration, each inmate is allowed to register from one (1) to twenty (20) telephone numbers. The facility will determine the maximum number of telephone numbers each inmate is allowed to register. Registration of a telephone number includes the number, name of the party who the inmate wishes to call, and the relationship of that party to the inmate.

The PAN Editor provides options to mark a selected PAN entry as Free, Blocked, Private, or Watched and includes a Line Information Data Base (LIDB) option which automatically validates the PAN entry number associated with the selected inmates PIN number to verify that the phone number is a valid number.

The telephone numbers registered by each inmate are identified with the inmate's PIN and are resident in the system.

5.06
Restrictions and Fraud Control Options

5.06.1 The proposed ITS shall allow DOC personnel to temporarily restrict or disconnect service to an individual inmate telephone or station, groups of telephones, or an entire DOC facility. The Proposal shall describe how this is accomplished with the proposed ITS system.

☑ **SECURUS has read and will comply.**

In the Secure Call Platform, authorized users can easily shut down a phone or group of phones. After logging on, the user would select the Admin functions, navigate to the General tab. From this screen, the user could select all phones, a group of phones, or an individual station. The system would indicate whether each phone was Enabled or Disabled. To shut down the phone, the user would select Disable. The phone would then be disabled in real-time.

5.06.2 In order to limit possible telephone fraud, a fraud prevention feature shall be available, which shall randomly interject pre-recorded announcements throughout the duration of the conversation to the called party and caller indicating the source of the call. The Proposal shall describe, in detail, how this feature is accomplished. The announcement pattern and content are subject to DOC approval and will not permit either calling party to talk while the announcement is being made.

☑ **SECURUS has read and will comply.**

SECURUS' system has the capability to utilize a periodic "voice overlay announcement" during inmate conversations.

The Secure Call Platform is capable of providing message prompts in English and Spanish. An inmate may select a specific language at the beginning of the call process by dialing a SINGLE DIGIT. This will initiate the selected language prompts to the inmate. If desired, the language selection for the called party may be present in the system database. If additional languages are required, they may be developed for specific customer needs, up to 12 additional languages. Voice overlay messages may be played throughout the call as an additional fraud protection feature. They can easily be customized to meet the needs of the Alaska DOC. This feature is programmed into the system, per customer specifications, prior to installation and adjusted as required. The volume of the voice overlay can be adjusted at any level to either disrupt or not

disrupt the inmates' conversation. The frequency that the established message is played may be programmed by minute increments or a random setting.

5.06.3 The proposed ITS shall be able to detect the called party's attempt to initiate a "3-Way" or "Conference Call" with a third party and immediately terminate and/or flag the call. The Proposal shall describe how this detection is accomplished with the proposed ITS system and provide the actual "field tested" percentage of successful attempts in using this feature.

☑ **SECURUS has read and will comply.**

SECURUS' inmate system will be capable of detecting and eliminating (minimizing) efforts to "transfer" inmate calls to a third party utilizing "3-Way calling" and/or "conferencing". Detection of any attempt by the called party to transfer an inmate call or to create a conference call will result in the call being disconnected. SECURUS' 3-Way and conferencing prevention feature(s)/technology are described below.

SECURUS will provide the Alaska DOC with the most robust and most effective switch-hook 3-Way call detection technology in the industry today. SECURUS is acknowledged as the undisputed leader in this field. Our research and development commitment has resulted in valued intellectual property, including the following 3-Way call detection patents:

- **U.S. Patent #5,319,702 Methods and Apparatus for Detecting and Responding to Hook Flash Events Occurring on a Remote Telephone**
- **U.S. Patent #5,539,812 Method an Attempted 3-Way Conference Call on a Remote Telephone**
- **U.S. Patent #5,805,685 3 Way Call Detection By Counting Signal Characteristics**
- **U.S. Patent #5,796,811 3 Way Call Detection**

An excellent example of our technological superiority is our continued development and perfection of 3-Way call detection. Around 1992, the introduction of 3-Way calling as a feature available by most local telephone companies created a problem for prisons and their need restrict inmates from accessing numbers the facilities had determined that should be blocked from inmate access. 3-Way calling also prevented prisons from having an accurate record of the inmate's telephone contacts, which created substantial security concerns. SECURUS, through our wholly owned subsidiary T-NETIX, was the first inmate call processing company to develop a solution to 3-Way calling using our now patented (US Patent Number 5,319,702) methodology.

Simply having the best 3-Way call detection in the industry was not enough for SECURUS. We have continued to research this issue and develop enhancements to our solution. Recent advancements in our 3-Way call detection methodology have led our customers to tell us they believe our 3-Way

detection was operation nearly flawlessly. This led SECURUS to commission an outside firm in the 4th quarter 2006, SIBRIDGE consulting, an independent consultancy, to verify the accuracy of the 3-Way call detection feature.

The SIBRIDGE study collected and audited call recordings and event logs for approximately 6,000 calls. This independent test of our new 3-Way calling detection capability revealed SECURUS' overall success rate to be in the mid to high nineties, most significantly the system accurately detected and prevented illegal 3-Way call attempts 96 percent of the time.

Selective Programming
Additionally, our 3-Way detection feature can be enabled according to classes of service, meaning facilities can choose whether to employ 3-Way prevention globally, or they can disallow 3-Way calling for specific phones, groups of phones or PINs.

5.06.4 The ITS shall have a call alert feature. This feature shall alert DOC personnel that a designated inmate is placing a telephone call to a specific number that has been assigned alert status or information on a "hot number" list has been received. DOC personnel at DOC's discretion shall activate this status. The Proposal shall describe how this feature will function.

☑ **SECURUS has read and will comply.**

The system enables facility personnel, with password authorization, to 'tag' specific dialed numbers or "hot numbers" from administrative stations. This feature will provide notification when those 'tagged' parameters are detected in the process of a call. The system will notify personnel immediately at all administrative stations that a call is being made to a "hot number" and will display the called number and location where the call is being made from on the administrative workstation screen.

The system is equipped with a remote call-forwarding feature for those numbers that are under surveillance by the investigative unit. The Covert Alert feature allows authorized personnel to monitor a call, from any designated remote location, while the call is in progress. Once a number, or PIN, is assigned a 'covert' status, the user simply enters a telephone number (cellular, home, office, etc.) to which he/she wants the call sent for 'Live' monitoring. The call is then automatically re-routed once the call is accepted by the called party and in progress. There are no distance barriers to the retrieval process so the remote telephone number can be located within the facility or across the country. As an additional benefit, administrators may continue to monitor other calls, through the on-site workstation, while utilizing the 'Covert Alert' remote live call-forwarding feature.

5.06.5 If a called party wishes to be added to an inmate's restricted call list or wishes to be on a list that will not allow reception of calls from any inmate in any institution, the ITS equipment shall have a feature to activate this function. Activation will be by either responding to voice prompts using the dual tone multi frequency (DTMF) telephone buttons or by responding with answers by voice. The system administrator shall have the capability to manage the list (see Section 5.05.10). This function shall have a verify capability.

☑ **SECURUS has read and will comply.**

The SECURUS Secure Call Platform is designed with global and individual restriction call list tables of called party telephone numbers. Personal Allowed Numbers (PAN) can be maintained per inmate PIN by a site administrator or automated by scheduling system refresh intervals of the PAN list. When using the automated system refresh method, the called party is provided the option to accept or refuse activation during the first call via use of the DTMF keypad. If the called party refuses to accept the call, the number is never entered into the PAN list. Additionally, once a number is on a PAN list, our patented PERMAblock feature permits end users to have the capability of blocking their number from future calls during call set up and will be blocked for all inmates within an institution.

5.06.6 The Proposal shall describe all detection and prevention capabilities related to fraudulent, illicit or unauthorized activity available on the proposed ITS.

☑ **SECURUS has read and will comply.**

Fraud Detection Data Analysis
The Secure Call Platform is continuously analyzing call data and system parameters to detect any system anomalies, hardware failures, fraud indications, lowered revenue levels, or unusual usage patterns. All telephone activity is logged and statistically analyzed to detect any attempts at 'Hookswitch Dialing', 'Black Boxing', 'Hacking', or any other fraudulent telephone activities.

Alerts
This feature enables facility personnel with password authorization to 'tag' specific dialed numbers or PINs that will provide notification when those 'tagged' parameters are detected in the process of a call. The system provides multi-level alerts that can be assigned to appropriate investigative groups. Real time alerts can be generated through the use of the phone system monitor. Otherwise there are various inmate reports available under the correctional WebManage application that can be used to notify the appropriate investigator wherever they reside within the network.

Second Dial Tone/Anti-Chain Dialing

The system does not allow an inmate to obtain a second dial tone without termination of the first call. Follow-on, or "chain" dialing, is prevented by a combination of features. When the called party disconnects prior to, or without the inmate hanging up, the Public Switched Telephone Network (PSTN) should by today's standards not return a "second" dial tone. Instead, a pre-recorded message such as "If you would like to make a call, please hang up then place your call," will be played to the inmate. Since not all Local Exchange Carriers implement this standard, the system uses the SECURUS patented 3-Way Call Detection System, plus standard battery, dial tone, and DTMF detection, to detect the called party's on-hook condition.

The Secure Call Platform constantly monitors the hookswitch of the inmate telephone. If the hookswitch is depressed at any time, internal dial tone will reappear. This prevents hookswitch manipulation for fraudulent purposes and prevents dialing if secondary dial tone is received after the called party hangs-up. Should an on-hook transition be missed by the system, the system continuously looks for the occurrence of DTMF tones and dial tone. After proper timing qualification of these tones, to prevent inadvertent disconnects due to ambient background noise, the system will cause call termination resulting in the re-establishment of either PIN tone, or dial tone to the inmate, forcing a new, fully-controlled call.

Extra Dialed Digits

The Secure Call Platform has incorporated a successful fraud control feature that prohibit additional 'digit dialing' and thus, thwarts any dial around attempt by the inmate. Once the inmate has entered the destination number, it is immediately processed through our validation system. If at all during the process the inmate attempts to dial additional digits, his/her call will be immediately terminated and the event will be logged by the Secure Call Platform.

Pattern Dial Detection

The Secure Call Platform can detect many dialing patterns, which might be attempts at fraud. Several numbers that are dialed in sequence, for instance, would alert the user that a possible fraud attempt is in progress. Secure Call Platform can also be configured to disallow additional digit dialing once the inmate has completed his dialing sequence. When an inmate attempts to dial more digits than necessary the system will simply disconnect the call.

Constant Fraud Controls

The system uses an automated operator exclusively. When a call is processed, any unnecessary dialing or hookswitch activity results in termination of the call, thereby eliminating potential fraudulent activities such as credit card calls and fraudulent use of calling card numbers. These control features are the result of the system's ability to control all aspects of the call process including providing

its own line voltage to the inmate station, isolating it from direct connectivity to a local telephone company.

Dialing Controls
The Secure Call Platform has incorporated a successful fraud control feature that prohibits additional "digit dialing" and thus, thwarts any dial around attempt by the inmate. Once the inmate has entered the destination number, it is immediately processed through our validation system. If at all during the process the inmate attempts to dial additional digits, his/her call will be immediately terminated.

Random Tag Lines
Professionally recorded voice prompts, featured by the system, all for specific call progressions and requirements. When monitoring and recording a voice prompt informs both parties that the call is being recorded and may be monitored by department personnel. In cases where time restrictions are placed on inmate calls, both the inmate and called party are warned one (1) minute prior to termination of the call. Customized random tag lines are also available as a precautionary measure to deter fraudulent use of phone. Voice prompts are easily manipulated and can be customized to meet the facility's wishes.

Call Validation
Call Validation—SECURUS employs the most sophisticated intelligent validation network in the industry. As a real-time, computer based switching system it never allows an inmate to be connected to a conventional dial tone. Each dialed number is thoroughly analyzed before the call is allowed to process. This includes determining if the area code and exchange are valid, checking the number against any restrictions such as customer requested blocks, and verifying through the national Line Information Data Base (LIDB) that the number is able to receive collect calls, and is not a cellular or pay phone, pager, etc. Once the dialed number passes all these tests it will be dialed by the system.

SECURUS currently serves approximately 2,900 inmate facilities with out validation hub. This collective information/validation process is very effective in reducing fraudulent and illicit calling.

Name Auto Insert
Using the Profiler PIN Application, the system offers an auto insert feature that records the inmate's name the first time the PIN is used. The recording is then filed and used each time the inmate places a call, thus eliminating any "window of opportunity" to pass call messages. This feature also can be used as a fraud deterrent ensuring that adequate funds are available.

Call Branding
Call Branding—Personalized prompts that identify the facility on each attempted call will be included with the system. Random tag lines are also available as a precautionary measure to deter the fraudulent use of phones. Further security

parameters may be set in place by allowing only prerecorded names to be used every time an inmate makes a call.

Frequently Called Number Report
The Frequently Called Number Report allows investigators to generate a report based on user-defined threshold criteria. For example, by entering "50" in the parameter field the system will display only those numbers that have been called 50 or more times within a designated time frame. Once the report is displayed on screen a simple click of the mouse will automatically produce a second report that represents all areas of the facility from which a specific number has been called. From this report investigators can analyze data to determine specific call patterns, detail suspicious activity and selectively assign a watched number status to potential fraudulent numbers.

5.06.7 The Proposal shall identify specific activities the proposed system capabilities shall detect and/or prevent. The Proposal shall also identify possible methods inmates may use to circumvent these capabilities.

☑ **SECURUS has read and will comply.**

Fraudulent Activity Attempted by Inmate	SECURUS ITS Detection and Prevention Feature	Prevention to Halt Inmate Circumvention Attempts
Unlawful Message Passing	Recording and Monitoring System	The inmate may attempt to pass messages before the call is accepted, speak softly or listen for a line noise indication that his or her call is being monitored. The ITS talk paths are muted before call acceptance, Digital recording and volume controls allow exceptional line monitoring capabilities. When monitoring is invoked, the system incorporates analog suppression/amplification hardware that allows investigative monitoring of calls without inmate or called party detection. There is absolutely no click noise, dB loss or other indicator when this feature is activated.
Unauthorized use of PINs	SECUREvoice ™ System	Inmates may attempt to use another prisoner's PIN to make unauthorized calls. SECUREvoice ™ halts this activity by requiring the inmate's voice print to be identified with the PIN before a call can be processed. Supervised Voice Verification enrollment is a necessary step to initial enrollment process. Because of the precision of this voice print identification method, inmates are unable to assume another inmate's voice identity when attempted.
Conference Calling to Unrestricted Line	3-Way Call Detection and Prevention Feature	The SECURUS Patented 3-Way Calling feature guards inmate attempts to create a connection to a conference call or transfer to an unrestricted outside line.

Fraudulent Activity Attempted by Inmate	SECURUS ITS Detection and Prevention Feature	Prevention to Halt Inmate Circumvention Attempts
Hook switching, Follow-On, Chain-Dialing, Black-Boxing, and Hacking	Second Dial Tone Prevention and Extra Dialed Digits Detection	The system combines the Second Dial Tone feature and Extra Dialed Digits feature to stop any form of Hook switching or Chain-Dialing attempts by through the systems own internal dial tone, detection of 3-Way calls, Extra dialed digits after a call has been accepted and DTMF tone monitoring. Thresholds may be programmed to disconnect calls as the system monitors these features.
Fraudulent Credit Card Calls or Calling Card Calls	Call Branding, Overlay Messages and Automated Operator	When inmates attempt to reach outside lines to commit fraudulent acts; called parties are protected by calls that identify the inmate at call acceptance and repeating overlay messages of where the prisoner is calling from through an automated operator only.
Extra Dialed Digits to Reach Unrestricted Line	Extra Dialed Digits Feature/ 3-Way Calling Detection	Once a call is accepted the inmate or called party may attempt to reach outside lines. The Extra Dial Digits and 3-Way Calling feature terminates calls immediately when the extra dialed digit threshold is met.
Harassment to Called Parties	Call Blocking	Programmed Call blocks will prevent inmates calling witnesses and others through facility programming and PIN programming capabilities. Called Parties may also permanently block calls by dialing the digit "5" on their keypad during call introduction.
Attempt to Call Unapproved Number	PIN System	In addition to the Call Blocking program parameters, the PIN system does not allow the inmate to call any number unless it has been pre-approved.
Message Passing Before Call Acceptance	Controlled Talk/ Listen Audio Paths & Recorded inmate name announcement	Inmates may attempt to pass messages before a call is accepted. However, the system prevents this activity by the controlled mute status of the phone line between the inmate and called party. Additionally, an inmate may try to state an unauthorized message instead of his or her name when the automated operator announces the call to the end user. To prevent this opportunity, the ITS uses the inmate's recorded name in the announcement message.
Attempt to Call a restricted or "HOT NUMBER"	Alerts Feature	Even when numbers are blocked in the system or restricted through the PIN system, inmates may attempt to circumvent these restrictions. The alerts feature, however, enables facility personnel with password authorization to 'tag' specific dialed numbers or PINs that will provide notification when those 'tagged' parameters are detected in the process of a call. The system provides multi-level alerts that can be assigned to appropriate investigative groups.

5.06.8 The proposed ITS shall be capable of detecting extra dialed digits from either the called party or the inmate's telephone. The Proposal shall describe the options available to DOC upon detection of the extra dialed digits (i.e., call termination, system alarm, or logging of call to the database).

☑ **SECURUS has read and will comply.**

The Call Control Processor incorporates sophisticated technology to identify specific activities and eliminate fraud attempts by providing the option to enable the Extra Dialed Digits (EDD) feature. This feature has the ability to detect additional DTMF digits that are dialed by the inmate and/or the called party after the dialed number has been entered to accept the call. The threshold of declaring an Extra Dialed Digits event is programmable for specific dialed numbers or on a facility-wide basis. The EDD feature provides extra protection against chain dialing fraud and terminates the call immediately if the EDD threshold is exceeded.

The Secure Call Platform system has incorporated a successful fraud control feature that prohibit additional 'digit dialing' and thus, thwarts any dial around attempt by the inmate. Once the inmate has entered the destination number, it is immediately processed through our validation system. If at all during the process the inmate attempts to dial additional digits, his/her call will be immediately terminated and the event will be logged by the Secure Call Platform.

5.06.9 The proposed ITS shall be capable of detecting unusual or suspicious number sequences dialed or dialing patterns that the system identifies as possible attempts to commit fraud. Proposal shall describe the options available to DOC upon detection of the unusual or suspicious number sequences.

☑ **SECURUS has read and will comply.**

Secure Call Platform can detect many dialing patterns, which might be attempts at fraud. Several numbers that are dialed in sequence, for instance, would alert the user that a possible fraud attempt is in progress. Secure Call Platform can also be configured to disallow additional digit dialing once the inmate has completed his dialing sequence. When an inmate attempts to dial more digits than necessary the system can simply disconnect the call.

There are three main actions the system might take in the event fraudulent activity is discovered during a call.

1. **Flag**
2. **Flag and warn**
3. **Flag, warn and disconnect**

For example; In the case of 3-Way detection, authorized personnel within the Alaska DOC can control these three actions by inmate, telephone and/or called party telephone number.

5.06.10 The system shall provide for telephone number blocking such as: Direct dialing, Operators, Information, Talk Lines, IXC Access, Toll Free Lines, Etc. Additionally, the unit shall allow for blocking of 11 digit numbers in order to prevent calling to:

Correctional Facilities
Correctional Facility Employees Homes
Judges and Prosecutors Homes
Emergency Numbers
Doctors Answering Service Numbers
Other facilities known to accept collect calls such as Hospitals, Telephone Companies, Unions, Etc

☑ **SECURUS has read and will comply.**

Call Blocking
During installation, a "Call Blocking" table is established which denies inmates from making calls to specific numbers. Access is denied to any number designated by the XXX.

The Secure Call Platform (SCP) is programmed to automatically prohibit calls to toll free, pay-per-call, directory assistance and emergency services, including: 800, 888, 877, 900, 976, 550, 555-1212, 700, 500, 911, 411, etc. Further, the Secure Call Platform automatically prohibit calls to all long distance carrier access codes including 10-XXX, 101-XXXX Primary Interstate Carrier (PIC) codes, all local numbers which access long distance carriers such as 950-XXXX and toll-free area codes and exchanges.

The Secure Call Platform has the capability to block virtually an unlimited number of calls at any one time. Number blocking is accomplished in one of three methods:

1. **Enter the number(s) to be blocked in the Restrict Number Editor through the on-site workstation, or**
2. **Submit the number(s) to be blocked to SECURUS**
3. **Our patented PERMAblock feature permits end users to have the capability of blocking their number via keystroke during call set up. This block will occur without Facility or SECURUS intervention.**

Either option provides for immediate restriction of the number once it is entered into the system. The Alaska DOC may submit a list of numbers they wish to have blocked and SECURUS will enter the numbers into the system prior to installation.

Call blocking can also be accomplished by the use of "wildcards". For example, using the NPA or NIP-NXX portions of the phone numbers, the system can be configured to block any number in the NAP or NPA-NXX range specified.

Because Call Blocking tables often contain thousands of entries, the Secure Call Platform offers virtually unlimited blocking potential with a capability of 10,000,000 individual entries. The entries may consist of an entire area code, an entire exchange code within an area code, or a specific telephone number.

This blocked number list may be administered locally by facility personnel using the Administrative Workstation, or remotely by the SECURUS National Service Center. All blocked numbers have an associated 'block' reason code that is stored in the blocked number database for future reference.

Additionally, the called party can use our patented PERMAblock feature to block their phone from receiving future calls by following the instructions of the voice prompts when the call is received and pressing the corresponding digit on their key pad to block their number.

3-Way Disconnect
SECURUS' inmate system will be capable of detecting and eliminating efforts to "transfer" inmate calls to a third party utilizing "3-Way calling" and/or "conferencing". Detection of any attempt by the called party to transfer an inmate call or to create a conference call will result in the call being immediately disconnected. As an option for investigative purposes the 3-Way call can be allowed to continue and be flagged. SECURUS' 3-Way and conferencing prevention feature(s)/technology are described below.

SECURUS will provide the ALASKA DOC with the most robust and most effective switch-hook 3-Way call detection technology in the industry today. SECURUS is acknowledged as the undisputed leader in this field. Our research and development commitment has resulted in valued intellectual property, including the following 3-Way call detection patents:

- U.S. Patent #5,319,702 Methods and Apparatus for Detecting and Responding to Hook Flash Events Occurring on a Remote Telephone
- U.S. Patent #5,539,812 Method an Attempted 3-Way Conference Call on a Remote Telephone
- U.S. Patent #5,805,685 Three Way Call Detection By Counting Signal Characteristics
- U.S. Patent #5,796,811 Three Way Call Detection

An excellent example of our technological superiority is our continued development and perfection of 3-Way call detection. Around 1992, the introduction of 3-Way calling as a feature available by most local telephone companies created a problem for prisons and their need restrict inmates from accessing numbers the facilities had determined that should be blocked from inmate access. 3-Way calling also prevented prisons from having an accurate record of the inmate's telephone contacts, which created substantial security concerns. SECURUS, through our wholly owned subsidiary T-NETIX, was the

first inmate call processing company to develop a solution to 3-Way calling using our now patented (US Patent Number 5,319,702) methodology.

Simply having the best 3-Way call detection in the industry was not enough for SECURUS. We have continued to research this issue and develop enhancements to our solution. Recent advancements in our 3-Way call detection methodology have led our customers to tell us they believe our 3-Way detection was operating nearly flawlessly. This led SECURUS to commission an outside firm in the 4th quarter 2006, SIBRIDGE consulting, an independent consultancy, to verify the accuracy of the 3-Way call detection feature.

The SIBRIDGE study collected and audited call recordings and event logs for approximately 6,000 calls. This independent test of our new 3-Way calling detection capability revealed SECURUS' overall success rate to be in the mid to high nineties, most significantly the system accurately detected and prevented illegal 3-Way call attempts 99 percent of the time.

5.06.11 Inmates are not allowed to call other DOC institutions or offices.

☑ **SECURUS has read and will comply.**

5.07
General Station Equipment (Telephone) Requirements

The Inmate Telephone Station Equipment required for DOC shall consist of 3 types of telephones. All telephone equipment shall be of the highest quality and shall be hearing aid compatible. The total number of telephone instruments for each facility is shown in Table One of this RFP. These totals are subject to change as the Department's needs change.

☑ **SECURUS has read and will comply.**

The first type, which shall be the majority of inmate telephones installed, shall be permanently mounted wall telephones meeting the specifications outlined in this Section of the RFP. The superintendent at each of the correctional facilities shall determine the quantity of this type of telephone, within the total number of telephones listed in Table One.

☑ **SECURUS has read and will comply.**

The second type of Inmate Telephone Station Equipment shall be portable or "movable" inmate telephones that are used mainly in segregation units and shall be manufactured to withstand abuse. The telephones can be cart mounted in areas where inmates can reach through bars to access the dialing pad or units compact enough to fit through standard cell door food slots where solid doors are utilized. Industry Standard 2500 telephone sets are not acceptable; The Proposal shall describe how these movable or portable telephones will be moved from one cell to another by DOC personnel to allow for inmate calling. The Offeror shall provide a

minimum of 1 of these instruments per special housing unit within each DOC facility. The superintendent at each of the correctional facilities shall determine the quantity of this type of telephones.

☑ **SECURUS has read and will comply.**

SECURUS is familiar with this type of requirement and has developed a portable unit that is of the same height to allow the handset of a secure inmate instrument the ability to fit through the Food Slot (Bean Hole).

SECURUS' portable telephones are mounted to prison carts or dollies. The Department personnel simply roll the device from one cell to another to allow for inmate calling.

The third type of Inmate Telephone Station Equipment shall be "all weather" inmate telephone sets to be used at DOC's discretion. The superintendent at each of the correctional facilities shall determine the quantity of this type of telephone.

☑ **SECURUS has read and will comply.**

5.07.1 All Inmate Telephone Station Equipment shall be of new manufacture latest technology and shall be provided with the proposed ITS at no cost to DOC. (See 5.07.3)

☑ **SECURUS has read and will comply.**

5.07.2 All Inmate Telephone Station Equipment shall be installed in all DOC institutions, at no cost to DOC.

☑ **SECURUS has read and will comply.**

5.07.3 The Offeror shall provide all required materials. Hardware/software and station cabling (where re-use is unavailable or new locations are required) to install the Inmate Telephone Station Equipment. **All materials provided shall be at no cost to DOC.**

☑ **SECURUS has read and will comply.**

5.07.4 All Inmate Telephone Station Equipment shall be powered by the telephone line and require no additional power source.

☑ **SECURUS has read and will comply.**

5.07.5 All Inmate Telephone Station Equipment shall have the physical and design characteristics that include all of the following:

- A chrome plated DTMF tone dial that is water, flame and shock resistant.
- A hearing aid compatible handset.
- A tamper proof steel housing that protects the electronic components of the telephone.

- A paint/finish that is mar and scratch resistant.
- A faceplate with concise dialing and operating instructions.
- An industry standard design.
- An armored handset cord that is resistant to stretching and breaking.
- A floating case hardened metal plate to prevent side drilling entry.
- An installation reinforced by security studs to prevent easy removal of the telephone.

☑ **SECURUS has read and will comply.**

SECURUS' Inmate Telephones are the strongest and most reliable units available, and are designed specifically for the prison environment. SECURUS provides the Wintel inmate telephone equipment.

The keypad is steel and the hookswitch has sealed contacts to resist environmental hazards and vandalism. The volume control may be technician set or may be controlled by an optional external button.

- **Powder Coated cold rolled steel provides rugged vandal resistant telephone housing designed and built for inmate use**
- **Heavy chrome metal keypad bezel, buttons, and hookswitch lever withstand abuse and vandalism**
- **Armored handset cord is equipped with a steel lanyard (1000# 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**
- **High impact, flame retardant, anti-vandal and anti-drill body (body must be constructed of materials that do not give off toxic gases when subjected to fire)**
- **Cord, approximately 3 foot armored or longer if requested**
- **Handset hearing aid compatible**
- **DTMF compatible**
- **FCC and UL approved with certification number**

5.07.6 The Proposal shall describe the handset cord component of the proposed Inmate Telephone Station Equipment including the lanyard used to connect the handset to the base telephone. It is preferred that this lanyard be a metal composition.

☑ **SECURUS has read and will comply.**

The armored handset cord is equipped with a steel lanyard (1000# pull strength) and secured with a 14 gauge retainer bracket for maximum vandal resistance.

5.07.7 The Inmate Telephone Station Equipment shall be compact in design. The Proposal shall include diagrams or photographs of the proposed Inmate Telephone Station Equipment.

☑ **SECURUS has read and will comply.**

Diagrams of the telephone equipment are included in *Attachment C – Equipment Specifications*.

5.07.8 The Inmate Telephone Station Equipment shall be true dual-tone multi-frequency (DTMF).

☑ **SECURUS has read and will comply.**

5.07.9 The Inmate Telephone Station Equipment shall not be programmable for any purpose.

☑ **SECURUS has read and will comply.**

5.07.10 The Inmate Telephone Station Equipment shall not include coin entry and return slots regardless of whether these functions are disabled.

☑ **SECURUS has read and will comply.**

5.07.11 The Offeror shall provide a unique number, physically imprinted on each Inmate Telephone Station Set so that DOC staff for the purpose of reporting troubles and troubleshooting problems can see the number. As the inmate Telephone Station Sets necessitate replacement, the Offeror shall number them. As new Inmate Telephone Station Sets are added or replaced they shall be identified in the same manner and all appropriate paper work shall be updated to reflect the addition.

☑ **SECURUS has read and will comply.**

5.07.12 The Inmate Telephone Station Equipment shall be capable of reducing background noise through the use of confidencers or directional microphones in the handset.

☑ **SECURUS has read and will comply.**

5.07.13 All Inmate Telephone Station Equipment shall provide volume controls that allow inmates to amplify the called party's voice.

☑ **SECURUS has read and will comply.**

5.07.14 The Proposal shall describe the provision of dialing instructions in multiple languages on each Inmate Telephone Station Set in a manner that reduces or eliminates the possibility of such instructions being destroyed. Labels or other accessible surface instructions shall not be acceptable.

☑ **SECURUS has read and will comply.**

Each Inmate Telephone Station dialing instruction plate will include dialing instructions in both English and Spanish on each Inmate Telephone Station Set that is printed and mounted behind a clear Lexan window, which is supported from behind by a metal plate and held securely in place at four points.

5.07.15 The Proposal shall describe the provision of a "warning" statement in multiple languages on each Inmate Telephone Station Set that states, "This Call is Subject to Monitoring and/or Recording" in a manner that reduces or eliminates the possibility of such statement being destroyed. Labels or other accessible surface instructions shall not be acceptable.

☑ **SECURUS has read and will comply.**

Each Inmate Telephone Station dialing instruction plate will include a "warning" statement in both English and Spanish on each Inmate Telephone Station Set that states "This Call is Subject to Monitoring and/or Recording" that is printed and mounted behind a clear Lexan window, which is supported from behind by a metal plate and held securely in place at four points.

5.07.16 The Offeror shall maintain the above-mentioned station set dialing instructions and warning statements for legibility and accuracy during the Contract term.

☑ **SECURUS has read and will comply.**

5.08
Voice Quality

5.08.1 The Offeror shall propose an ITS that provides a quality of connections that meets or exceeds appropriate current industry standards in the United States and enacted by appropriate standards organizations for transmitted and received levels, noise, cross talk and frequency range. The Offeror shall provide DOC with the standard (i.e., Bellcore and ANSI) to which its ITS will adhere.

☑ **SECURUS has read and will comply.**

The SECURUS' proposed ITS meets and/or exceeds all of the State and Federal industry standards for telephone reception and service quality. We will adhere to all applicable Bellcore, ANSI, and IEEE standards.

SECURUS uses full time EMI/RFI filters that prevent line noise from causing data errors and innovative line-interactive design that uses the DC to AC power

inverter "in reverse," like a battery charger, during normal operation providing greater performance and efficiency.

SECURUS utilizes state-of-the-art telecommunications equipment to provide acceptable audio quality well within the guidelines of Bellcore and ANSI standards. Specifically, SECURUS maintains an audio frequency response of +/1 .1dB, 300-3400Hz (relative to 0 dBm, 1000Hz). Extensive testing is performed, including numerous test calls from each facility during installation, to ensure excellent audio quality. All work required to satisfy this requirement will be done at no cost to the Alaska DOC. The lines utilized by the system are ordered through the local exchange carrier (LEC), which guarantees equivalent audio quality.

SECURUS provides P.01 (one caller out of 100 will be blocked), or better, level of service. SECURUS utilizes state-of-the-art electronic equipment, and digital recording and T1 equipment to provide acceptable audio quality, at a minimum. SECURUS does not use voice compression, and maintains an audio frequency response of +/-.1dB, 300-3400Hz (relative to 0 dBm, 1000Hz). Extensive testing is performed, including numerous test calls from each facility during installation, to ensure excellent audio quality and dial tone availability.

A P.01 Grade of Service (GOS) is "the probability (P), expressed as a decimal fraction that one call out of one hundred, during the average busy hour, will be blocked." It is in the best interest of SECURUS to complete as many calls as possible. Therefore, all systems have immediate automated reporting that shows when a call was unable to be completed due to a busy condition. In the event call traffic increases and the GOS falls below P.05, SECURUS will install additional lines to the Calling Platform at no cost to the State.

5.08.2 The voice quality level listed above shall be in place for all telephone services at all stages of a call and shall not be affected by any other ITS feature, function or capability.

☑ **SECURUS has read and will comply.**

5.09
Americans with Disabilities Act (ADA) Compliance

All of the proposed ITS station sets shall be ADA compliant. Due to security concerns, DOC shall be capable of requiring the Contractor to modify certain features on station sets such as cord length and mounting height. The ITS' TDD/TTY equipment shall be protected and secured by DOC when not in use.

☑ **SECURUS has read and will comply.**

5.09.1 All of the Inmate Telephone Station Equipment shall be compatible with telecommunications for the deaf (TDD/TTY) equipment.

☑ **SECURUS has read and will comply.**

5.09.2 The Offeror shall be responsible for providing a single TDD/TTY device for the ITS at each DOC institution listed in Attachment A of this RFP. More than one said device may be required if the institution has 10 or more inmates that require TDD/TTY equipment.

☑ **SECURUS has read and will comply.**

5.09.3 The ITS TDD/TTY equipment shall be portable, such that it can be used with any ITS
station set at each DOC institution listed in Table One of this RFP.

☑ **SECURUS has read and will comply.**

The SECURUS TDD portable units feature-direct connect. Call progress tells the inmate if the phone he or she is calling is ringing or busy. Convenient arrow keys make it easy to review information saved in memory. The TTY Announcer lets hearing people know the inmate is on the line. The User-programmable Relay Voice Announcer tells hearing callers to use a TTY or use relay, and gives the phone number for the inmate's relay service. Auto ID lets everyone you call know that the inmate caller is using a TTY.

Superprint 4425 Portable TDD

- **· Built-in, 24-character printer**
- **· 3 selectable print sizes**
- **· 32k memory**
- **· Date/time printed at the beginning of each call**
- **· Turbo Code® and Auto IDTM**
- **· Built-in ring flasher**
- **· Arrow keys for easy review of memory**
- **· Convenient GA/SK keys**
- **· Easy-touch greeting memo**
- **· Baudot code (45.5/50 baud rate)**
- **· Sticky key feature (for single-handed typing)**
- **· ASCII code is available**
- **· Model CT-178ADP**
- **· FCC Registered: 1U8USA-74411-CC-T**
- **· TTY AnnouncerTM tells hearing callers you are using a TTY**

Additional TDD Features Include:

- **· Direct connect (with 2 jacks) to standard telephone line**

- **· User-programmable Relay Voice Announcer**
- **· Call progress - display indicates "ringing" or "busy"**
- **· Auto-Answer capabilities (with programmable message)**
- **· Auto-busy redial and Wait for Response**
- **· Remote message retrieval**
- **· Tone or pulse dial**
- **· Keyboard dialing**
- **· Memory dialing/redial**

5.09.4 The ITS TDD/TTY equipment shall allow inmates to communicate via keyboard entry.

☑ **SECURUS has read and will comply.**

5.09.5 The ITS TDD/TTY equipment shall contain a display (i.e., LCD and LED) and a printer device.

☑ **SECURUS has read and will comply.**

All TDD/TTY equipment will contain a digital display (i.e., LCD and LED) and a printer device. The display shows call progress and tells the inmate if the phone he or she is calling is ringing or busy. Convenient arrow keys make it easy to review information saved in memory within the display.

5.09.6 The ITS TDD/TTY equipment must have real-time monitoring capability so that whatever is keyed is immediately displayed at a remote monitoring area or site. Mike Hammond

☑ **SECURUS currently does not have the capability to display what it typed on the Alaska DOC monitor. We have the capability to record and monitor the audible conversation from either the called or calling party including the live TTY/TDD operator.**

5.09.7 The ITS shall record the entire call utilizing the TDD/TTY equipment.

☑ **SECURUS has read and will comply.**

5.09.8 The Offeror shall provide decoding and playback capability. The system shall not rely on paper copy only.

☑ **SECURUS is not aware of a device that will provide decoding capabilities. We have contacted our TDD/TTY equipment manufacturer and will continue to work toward that goal.**

5.09.9 A separate call-length timer shall be provided for the TDD/TTY service.

☑ **SECURUS has read and will comply.**

SECURUS can provide different call length timers for TDD/TYY devices.

5.10
Collect Call Services

5.10.1 The Offeror shall provide the collect call services required in this RFP through the use of an automated operator. An inmate shall never be connected to a "live" operator.

☑ **SECURUS has read and will comply.**

SECURUS' inmate system will utilize mechanized (electronic) operators.

The Secure Call Platform utilizes an automated operator system. At no time will inmates have access to a live operator.

5.10.2 The Offeror shall be responsible for billing parties receiving collect calls from the ITS and for collecting payments for these calls.

☑ **SECURUS has read and will comply.**

5.10.3 The Offeror shall provide a toll free number that will be clearly shown on the called party's bill for assistance in billing matters.

☑ **SECURUS has read and will comply.**

5.10.4 The Offeror shall provide all local, intraLATA, interLATA, interstate and international collect call services at all DOC institutions where the ITS is installed. The Offeror shall be responsible for installing and maintaining all telephone circuits necessary to provide the required collect call services.

☑ **SECURUS has read and will comply.**

5.10.5 The proposed ITS shall allow for collect calls to be placed to international locations outside of the 50 states and United States territories.

☑ **SECURUS has read and will comply.**

5.10.6 The Offeror's Inmate Class of Service **collect call rates** charged to the called party, within Alaska, regulated by the RCA, shall not exceed tariff per minute rates and tariff per call surcharges, applicable to intrastate/intraLATA toll and intrastate/interLATA calls originating from DOC facilities collectively, including surcharges, the "intrastate Tariff Rates." The called parties (individuals on the inmates' approved calling lists) pay a per call surcharge regardless of the duration of the call, in addition to specified per minute rates that vary based upon the type of call. The intrastate intraLATA per minute rates are mileage banded, date, and time-of-day-

sensitive. The Offeror shall provide a breakdown of its Intrastate Tariff Rates. The Offeror's Intrastate Tariff Rates shall remain fixed for the term of the Contract and not be changed without the DOC's written consent.

☑ **SECURUS has read and will comply.**

SECURUS has provided Intrastate Tariff Rates in the separate Cost Proposal as required.

5.10.7 The Offeror's rates charged to the called party for collect calls outside of Alaska, regulated by the FCC, shall not exceed the tariff per minute rate for collect long distance calls and shall not exceed the surcharge rate for Inmate Class of Service Operator Station Collect. The Offeror shall provide its interstate per minute rate and surcharge. The Offeror's interstate tariff rate and surcharge shall remain fixed for the term of the Contract and not be changed without the DOC's written consent.

☑ **SECURUS has read and will comply.**

SECURUS certifies by this statement that it complies with all Federal laws, FCC regulations and requirements pertaining to the provision of Interstate telecommunications services to confinement facilities. As these laws, regulations and/or requirements change, SECURUS revises its practices and procedures as needed to remain in compliance. SECURUS shall not exceed the per minute rate for collect interstate long distance calls or the per call surcharge rates agreed upon by Contract with the Alaska DOC. The interstate rates and surcharges shall remain fixed for the term of the Contract and shall not be changed without the DOC's written consent.

SECURUS has provided its interstate per minute rate and surcharge in the separate Cost Proposal as required.

5.10.8 The Offerer shall provide a percentage of the gross revenues for all calls. The percentage paid to DOC shall not be less than 50% of the gross receipts for all calls collect and long distance. The Offerer shall not deduct fraudulent, uncollectible or unbillable calls, Local Exchange Carrier (LEC) access, LEC or long distance usage, maintenance or any costs of running the ITS, from the gross revenues for all calls prior to paying the minimum 50% fee to DOC. In other words, the percentage rate shall be based on gross call cost including per call surcharges and per minute charges, not the net after expenses. The Offerer is responsible for collecting all revenue from the called party for collect calls billed. **Local calls from pre-trial booking phones must be free. Charges will apply to all other local calls.**

AMENDMENT NUMBER ONE:

The following changes/additions are required:

Change Section 5.10.8 of the RFP to read:

5.10.08 The Offeror shall provide a percentage of the gross revenues for all calls. The Offeror shall not deduct fraudulent, uncollectible or un-billable calls, Local Exchange Carrier (LEC) access, LEC or long distance usage, maintenance or any costs of running the ICS, from the gross revenues for all calls prior to paying the percentage rate to the DOC. In other words, the percentage rate shall be based upon gross call cost including per call surcharges and per minute charges, not the net after expenses. The Offeror is responsible for collecting all revenue from the called party for collect calls billed.

☑ **SECURUS has received and read the AMENDMENT NUMBER ONE changes and responded in the Cost Proposal as required.**

5.10.9 The Offeror's Rates for international calls shall be the current prevailing cost for international calls to the specific country being called.

☑ **SECURUS has read and will comply.**

5.10.10 A check for the commission amount for the collect-calling mode, shall be sent to DOC no later than 45 days after the close of the billing month. For example, a commission check for calls made during April shall be forwarded to DOC no later than June 15th. A summary report shall be provided with each commission check, that includes the following:

A. Total commission figure broken down by Institution; and

☑ **SECURUS has read and will comply.**

B. Listing of total minutes, total calls by Institution.

☑ **SECURUS has read and will comply.**

5.11
Miscellaneous Requirements

5.11.1 The Offeror shall not charge for calls that result in Special Information Tones (SIT), ring/no answer, or busy conditions.

☑ **SECURUS has read and will comply.**

5.11.2 The Offeror shall provide local exchange service for collect calling use at each DOC institution listed in Table One of this RFP. Additionally, the Offeror shall provide local exchange service for prepaid calling use at each DOC institution listed in Table One of this RFP, pursuant to Section 5.29 of this RFP. The local calling area shall be equivalent to the local calling public pay telephone area at each DOC institution. The Offeror must assure that the proposed ITS is capable of identifying a dialed number as local, based on the pay telephone calling area, and correctly rate and route the call.

☑ **SECURUS has read and will comply.**

5.11.3 The Offeror shall install and maintain all telephone circuits necessary to provide local exchange and long-distance calling. All costs shall be the responsibility of the contractor.

☑ **SECURUS has read and will comply.**

5.12
ITS System Calling Protocols

5.12.1 Each call placed through the ITS must be electronically identified by the ITS system as being a call originating from "(name of institution), an Alaska correctional institution," with or without the accompanying inmate PIN. The ITS will provide options to the party called to accept the individual call, not accept the individual call, or not accept any calls from a correctional facility in the future.

☑ **SECURUS has read and will comply.**

Upon receiving a call from an inmate, the called party will hear an announcement similar to the following:

> ***"Hello, this is a collect call from "INMATE'S NAME", an inmate at the "Alaska DOC Correctional Facility". To accept charges press three (3); to refuse charges press five (5) or hang up now; to block your number from receiving calls from this facility, press six (6); to obtain a rate quote press four (4)". After acceptance of call, "This call is subject to monitoring and recording. Thank you for using SECURUS".***

5.12.2 If a call is not accepted by the party called, or if no one answers the call, the Offeror's service shall inform the inmate of the situation and not simply disconnect the call.

☑ **SECURUS has read and will comply.**

The proposed ITS will allow an inmate to hear all call progress (i.e., ringing, busy, SIT, etc.) tones and messages when processing a call. The system will allow the inmate to hear the processing of the placed call to determine if a SIT with message or an answering device (i.e., answering machine, voice mail, etc.) has answered the call. The system also provides very specific information to the inmate in the event a call is not completed. At no time will the system allow the inmate to speak (restricted voice channel) until the called party has accepted the call.

This is a result of the integration between SECURUS' validation system and the calling platform. Examples of the voice prompts provided to the inmates if a call was not completed are as follows:

- **"That number is restricted"**
- **"The number you have dialed has a collect call block"**

- **"Try your call again at a later time"**
- **"That is not a valid number"**
- **"This call is being terminated, dialing of additional digits is not allowed"**
- **"No calls are allowed at this time"**
- **"Your call was refused"**
- **"All circuits are busy"**
- **"No one is answering at this time"**
- **"No third party or credit card calls are allowed"**
- **"You have reached your maximum allowed number of calls" (PIN/debit).**

5.12.3 The ITS must have the capability to accept the called party's response via Dual Tone Multi-Frequency (Touch Tone Pad) input from the telephone. The Proposal shall describe how the ITS system will accept input from rotary dial telephone users.

☑ **SECURUS has read and will comply.**

For called parties using rotary phones, the system utilizes a sophisticated rotary-dial detection algorithm that provides a robust method of digit detection for this older generation of telephones.

Specific dialed numbers may be programmed to allow for Rotary Acceptance. The called party still receives the same acceptance message and call restrictions that are implemented on a touch tone acceptance call. At present less than .02 percent of all called numbers are programmed for Rotary Acceptance.

5.12.4 The ITS shall have the capability to accept the called party's response via voice response. (Yes/No Response)

☑ **SECURUS has read and will comply.**

The called party, upon receiving a call from an inmate, the called party will hear an announcement similar to the following:

> **"Hello, this is a collect call from "INMATE'S NAME", an inmate at the "Alaska DOC Correctional Facility". To accept charges press or say three (3); to refuse charges press or say five (5) or hang up now;**

5.12.5 The ITS shall have the capability to interject messages into a telephone call at random intervals (i.e., "this call is from an Alaska correctional institution") as deemed necessary by DOC and at DOC determined intervals. The content is subject to approval of DOC. This feature must be capable of being heard over and above the caller or called party voices when interjected. The correctional institution must control

the activation or deactivation of this feature.

☑ **SECURUS has read and will comply.**

Voice overlay messages may be played throughout the call as an additional fraud protection feature. The actual prompt can easily be customized to meet the needs of the Alaska DOC. This feature is programmed into the system, per customer specifications, during installation or added anytime during the contract. Activation of this feature will be mandated by each institution upon request. Request is made through the system administrator or by simply initiating a service ticket through the SECURUS technical support help desk. The volume of the voice overlay message prompt is adjustable and will be at a level that meets the requirements of the Alaska DOC. The frequency that the established message is played may be programmed by minute increments or a random setting.

5.12.6 The ITS shall be capable of announcing to the called party the name of the calling inmate. Offerors shall provide a mechanism to record an inmate's name one time to be used each time this announcement is required. The correctional institution must control the activation or deactivation of this feature.

☑ **SECURUS has read and will comply.**

Upon receiving a call from an inmate, the called party will hear an announcement similar to the following:

> ***"Hello, this is a collect call from "INMATE'S NAME", an inmate at the "Alaska DOC Correctional Facility". To accept charges press three (3); to refuse charges press five (5) or hang up now; to block your number from receiving calls from this facility, press six (6); to obtain a rate quote press four (4)". After acceptance of call, "This call is subject to monitoring and recording. Thank you for using SECURUS".***

The system provides a mechanism to record an inmate's name one time to use each time this announcement is required. The announcement wording is controlled by the Alaska DOC.

5.13.7 The ITS shall be capable of announcing to the called party how to accept collect calls. The correctional institution must control the activation or deactivation of this feature.

☑ **SECURUS has read and will comply.**

Upon receiving a call from an inmate, the called party will hear an announcement similar to the following:

> ***"Hello, this is a collect call from "INMATE'S NAME", an inmate at the "Alaska DOC Correctional Facility". To accept charges press three (3); to refuse***

charges press five (5) or hang up now; to block your number from receiving calls from this facility, press six (6); to obtain a rate quote press four (4)". After acceptance of call, "This call is subject to monitoring and recording. Thank you for using SECURUS".

The activation or deactivation of this feature is controlled by the Alaska DOC.

5.12.8 The ITS shall be capable of announcing to the called party the collect call rate, prior to acceptance.

☑ **SECURUS has read and will comply.**

Upon receiving a call from an inmate, the called party will hear an announcement similar to the following:

"Hello, this is a collect call from "INMATE'S NAME", an inmate at the "Alaska DOC Correctional Facility". To accept charges press three (3); to refuse charges press five (5) or hang up now; to block your number from receiving calls from this facility, press six (6); to obtain a rate quote press four (4)". After acceptance of call, "This call is subject to monitoring and recording. Thank you for using SECURUS".

5.13
ITS System Call Recording and Monitoring

5.13.1 The ITS shall be capable of recording all inmate calls simultaneously and at any time that a call is placed. The Proposal shall describe how such recording will be accomplished with the proposed ITS system including the type of equipment and software being used.

☑ **SECURUS has read and will comply.**

SECURUS is the manufacturer of the Secure Call Platform offered in this response. The ability to record all conversations simultaneously is a standard feature of Secure Call Platform designed and manufactured by SECURUS Technologies. No other hardware or software is required to link, connect or integrate to offer recording of inmate conversations. SECURUS has been offering "built in" recording of our products since 1993 and will continue to do so as part of the Alaska DOC centralized recording requirement.

The Secure Call Platform is capable of recording all calls simultaneously and also allows personnel to listen to a pre-recorded call, while active calls continue to be recorded—all without loss of information. The system records the entire conversation from the time of positive acceptance to termination of the call. Because the recording and monitoring applications are fully integrated features of the system, call synchronization between call record time and recording time is guaranteed.

The system enables facility personnel to listen to a conversation in-progress on a real-time basis and have the conversation recorded at the same time. All conversations currently in progress will be displayed and the user may select the desired conversation to monitor. Once the user makes the selection, the requested conversation will be directed to the integrated playback module.

The proposed ITS enables the system administrator to select specific dialed or called numbers, inmate telephone set or lines, and calls place using specific inmate PINs to be recorded. When the platform detects activity based on the selected criteria, conversations will be automatically recorded. As an alternate mode of operation, the platform will simultaneously record all inmate conversations.

5.13.2 The recording feature shall be capable of being de-activated on a per number dialed and/or per PIN basis.

☑ **SECURUS has read and will comply.**

The recording feature is capable of being de-activated on a per number dialed basis within the Global Editor of the Secure Call Platform. The user would enter a dialed number, and select a checkbox marked Recording, or deselect the checkbox to prevent recording.

5.13.3 The proposed ITS shall allow DOC personnel to monitor inmate calls while in process ("real time"). This monitoring shall be by specific inmate telephone or station. Any equipment and software required to perform this function shall be provided with the proposed ITS system.

☑ **SECURUS has read and will comply.**

The Secure Call Platform Live application allows for immediate, real-time monitoring of calls in progress via the multi-media PC workstation. Facility personnel (with appropriate password privileges) are able to monitor live calls by simply highlighting the call in progress and clicking on the speaker icon. This process is undetectable by either the inmate or the called party and does not disrupt the recording process. Furthermore, concise descriptions of activity are displayed for each phone in use, for example, the system displays the specific telephone location, inmate PIN and name (if option is used), the destination number dialed, city and state of the destination, time and duration of call, any restrictions such as "Watched" or "Private", and the status of the call, such as "In Progress," "Calling Destination," "Get Acceptance".

The platform also provides the ability to automatically eliminate any monitoring or recording of special calls, such as to legal counsel, by designating the number as a "private" number. In the event that a retrieval of a "private" call is attempted, the Secure Call Platform will inform the user that, *"This call is prohibited from monitoring."*

5.13.4 The proposed ITS shall allow live monitoring of inmate calls in progress and/or retrieve archived information from remote locations via telephone.

☑ **SECURUS has read and will comply.**

The call playback feature will allow 360 days of recorded calls for immediate retrieval and allow search and playback within 30 seconds. Corrections personnel can listen to live or archived recordings via multi-media PC interfaces connected over Local Area Networks (LANs). Multiple levels of security provide that only authorized personnel can access and monitor the inmate recordings. The audio may be directed to the integrated loudspeaker or headphones. This output may be also be used to record the conversation(s).

Recordings are played back using the SECURUS media control, accessible through the Web Browser and can then be stored to CD as needed by the Alaska DOC.

The SECURUS Secure Call Platform provides the capability to copy the conversations onto a compact disc (CD) or other storage device. Administrative terminals will be equipped with speakers and a CD R/W device to comply with this request.

Recorded calls can be transferred to a CD via the CD Burner function of the Secure Call Platform. There are three choices for CD format. Data CD is automatically selected, but you can select Data CD Encrypted requiring a password to play back a call or Audio CD for playback on any portable CD player.

***Data CD*—allows approximately 2,900 minutes to be saved to the CD. In addition to the call recordings, a program is saved to the CD that allows playback from any computer.**

***Audio CD*—allows approximately 80 minutes of calls to be saved to the CD. This CD plays just as any audio CD.**

For more on call monitoring, please refer to our responses to 5.13.3 and 5.13.5.

5.13.5 The proposed ITS shall allow for "real time" audible monitoring of inmate calls by specific inmate PIN entered by DOC personnel. The Proposal shall describe how this monitoring will be accomplished with the proposed ITS.

☑ **SECURUS has read and will comply.**

The Secure Call Platform Live application allows for immediate, real-time monitoring of calls in progress via the multi-media PC workstation. Facility personnel (with appropriate password privileges) are able to monitor live calls by simply highlighting the call in progress and clicking on the speaker icon. This process is undetectable by either the inmate or the called party and does not disrupt the recording process. Furthermore, concise descriptions of activity

are displayed for each phone in use, for example, the system displays the specific telephone location, inmate PIN and name (if option is used), the destination number dialed, city and state of the destination, time and duration of call, any restrictions such as "Watched" or "Private", and the status of the call, such as "In Progress," "Calling Destination," "Get Acceptance".

The system also provides the ability to automatically eliminate any monitoring or recording of special calls, such as to legal counsel, by designating the number as a "private" number. In the event that a retrieval of a "private" call is attempted, the Secure Call Platform will inform the user that, "This call is prohibited from monitoring."

Monitoring of inmate calls is provided in true "real time". The Department personnel will be capable of monitoring an inmate's call while the call is in progress with no delay in transmission of the audio.

The system enables facility personnel to listen to a conversation in-progress on a real-time basis and have the conversation recorded at the same time. All conversations currently in progress will be displayed and the user may select the desired conversation to monitor. Once the user makes the selection, the requested conversation will be directed to the integrated monitoring module.

The proposed ITS enables the system administrator to select specific dialed numbers, lines, or inmate PINs to be recorded. When the platform detects activity based on the selected criteria, conversations will be automatically recorded.

The alerts feature enables facility personnel with password authorization to 'tag' specific dialed numbers or PINs that will provide notification when those 'tagged' parameters are detected in the process of a call. The system provides multi-level alerts that can be assigned to appropriate investigative groups. The system will be equipped with the capability to bridge a call to an authorized remote number for those numbers, or hot PINs, that are under surveillance by the investigative unit. The Covert Alert feature allows authorized personnel to monitor a call, from any designated remote location, while the call is in progress. Once a number, or PIN, is assigned a 'covert' status, the user simply enters a telephone number (cellular, home, office, etc.) from which he/she wants the call sent to for 'Live' monitoring. The call is then automatically bridged once the call is accepted by the called party and in progress.

There are no distance barriers to the retrieval process so the remote telephone number can be located within the facility or across the country. As an additional benefit, administrators may continue to monitor other calls, through the on-site workstation, while utilizing the 'Covert Alert' remote live call-forwarding feature. This allows for facility investigators to effectively monitor potential elicit activities regardless of the investigators' location. If the investigator is unable to perform live monitoring as the result of a covert alert notification, the recordings remain available and will be identified with alert notification status.

5.13.6 The voice call recording system proposed with the ITS shall be a fully digital system utilizing a combination of hard drives and optical storage or other state-of-the-art digital drives. Systems utilizing magnetic tapes for voice call recording shall not be considered. The Proposal shall describe the type of voice call storage devices included in the proposed ITS system.

☑ **SECURUS has read and will comply.**

The Secure Call Platform's unique, fully integrated recording application, works independently of other product(s) so there is never a need for separate manufacturers' product to work along side the system. The Secure Call Platform employs large capacity hard drives along with RAID (Redundant Array of Inexpensive Disks) that virtually extend the call storage period and enhance system redundancy and call backup to meet your specific needs.

5.13.7 The proposed recording system shall be capable of capturing the conversation of both parties with equal level and quality.

☑ **SECURUS has read and will comply.**

5.13.8 The proposed recording system shall provide the highest quality playback possible by limiting compression as may be required. The Offeror shall assure the DOC that voice playback quality is not compromised by compression techniques and can be easily understood by someone who may not be familiar with the voice being recorded.

☑ **SECURUS has read and will comply.**

5.13.9 The proposed recording system shall have sufficient storage capacity to record and maintain all voice calls for 1 year. The Proposal shall demonstrate that 1 year of calls can be maintained by the use of graphs and charts.

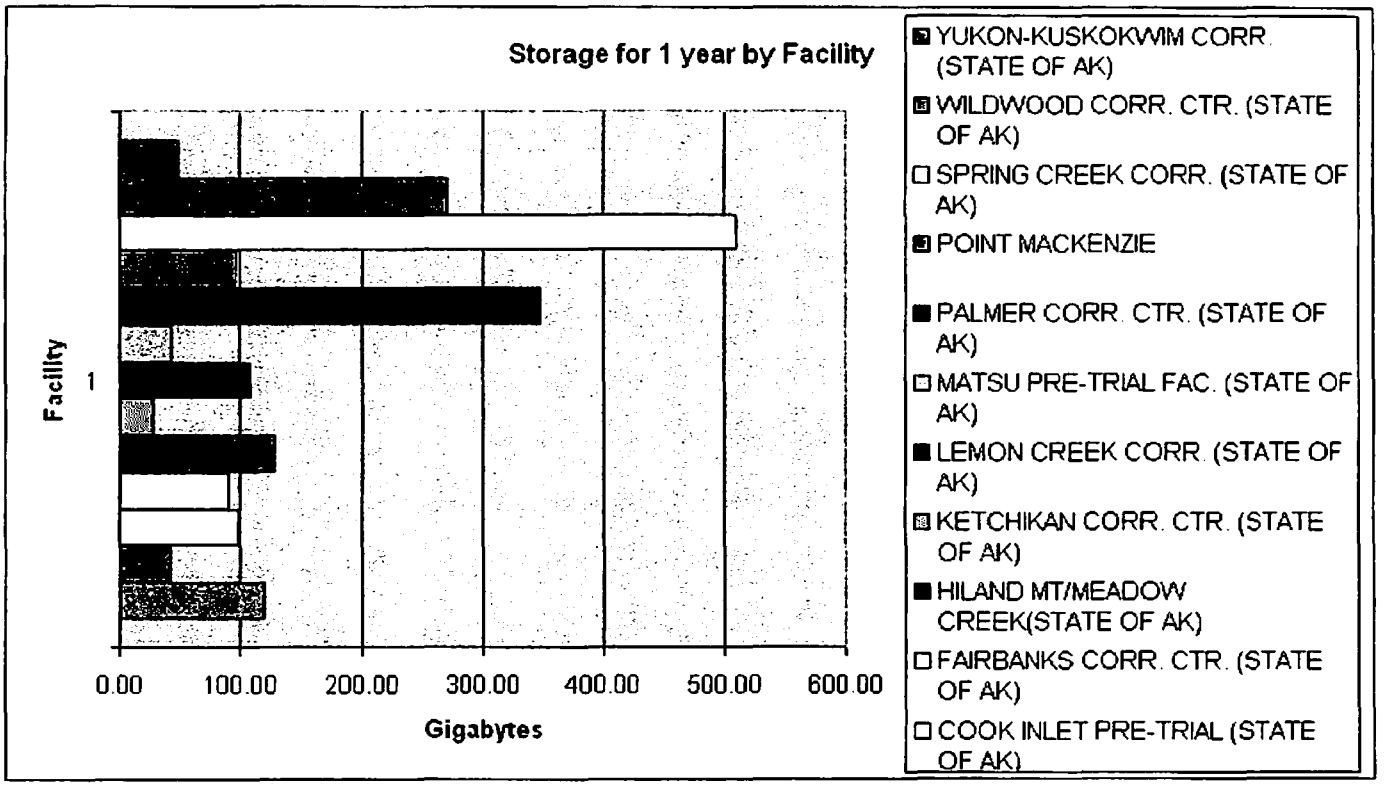
☑ **SECURUS has read and will comply.**

Call recording (on-line and archived) are centralized in a Class IV disaster resistant carrier class data center that is managed under the direct supervision and immediate hands on maintenance of data center personnel.

The call recordings are initially stored for on-line retrieval on multiple Redundant Arrays of Independent Disk (RAID) in two separate Storage Area Networks (SAN). All recordings are written twice to each of the SAN units promoting disaster recovery in the event of single disk or entire RAID failure.

Archiving is automated and managed by robotic tape drives. No intervention required by facility to manage tape or archiving libraries. Access to archived recordings will take approximately 30 seconds for the Oracle database to identify the location of archived call, retrieve tape, insert tape in tape drive and move to on-line availability.

Alaska DOC Call Duration History from 200605 to 200704 Intra In State Sum of Duration	Minutes for 1 year storage	Space in GB +25% growth
ANCHORAGE JAIL (STATE OF AK)	191,450	119.66
ANVIL MOUNTAIN CORR. (STATE OF AK)	66,531	41.58
COOK INLET PRE-TRIAL (STATE OF AK)	155,894	97.43
FAIRBANKS CORR. CTR. (STATE OF AK)	144,156	90.10
HILAND MT/MEADOW CREEK(STATE OF AK)	203,787	127.37
KETCHIKAN CORR. CTR. (STATE OF AK)	44,402	27.75
LEMON CREEK CORR. (STATE OF AK)	171,657	107.29
MATSU PRE-TRIAL FAC. (STATE OF AK)	69,333	43.33
PALMER CORR. CTR. (STATE OF AK)	555,362	347.10
POINT MACKENZIE	155,576	97.24
SPRING CREEK CORR. (STATE OF AK)	815,619	509.76
WILDWOOD CORR. CTR. (STATE OF AK)	431,982	269.99
YUKON-KUSKOKWIM CORR. (STATE OF AK)	77,687	48.55
Total	**3,083,436**	**1927.15**



5.13.10 In the event that voice calls are required to be stored (i.e., court order) beyond the 6- month interval; such calls shall be tagged and saved.

☑ **SECURUS has read and will comply.**

It may be useful to group several calls together if they pertain to the same case or investigation for long term access. Secure Call Platform allows a user to create a record of an investigation and store pertinent calling information there. Once an investigation has been created, you can attach recorded calls to it from the Call Detail Report and burn calls to CD's for long term storage beyond the 6-month on-line storage period.

5.13.11 In the event that voice retention requirements are increased beyond the 6-month interval, selected equipment shall have the capability without replacement, to meet new storage requirements.

☑ **SECURUS has read and will comply.**

5.13.12 Workstations and related peripheral requirements are described in Section 5 of this RFP. The Offeror shall include good quality speakers and headsets with each workstation for the best quality playback. The Proposal shall describe the quality of the speakers.

☑ **SECURUS has read and will comply.**

Engineered for superb sound and styled for ultimate convenience, the Dell™ A225 two-piece stereo speaker system delivers a perfect combination of performance and value in a smart, well-designed form. This USB powered system delivers up to 1.2 W total RMS output power and includes two speakers that can be placed on either side of your monitor. The system features volume control with on/off switch on one speaker. With features that include rich, full sound and great convenience, these ROHS-complaint speakers make a perfect audio companion. This product has been tested and validated on Dell™ systems to ensure it will work with your system and is compatible with select Dell™ OptiPlex™ Desktop / Precision™ WorkStation Systems. It is supported by Dell™ Technical Support when used with a Dell™ system.

- **2 Speaker System**
- **USB powered**
- **1.2 W total RMS output power**
- **ROHS-complaint**

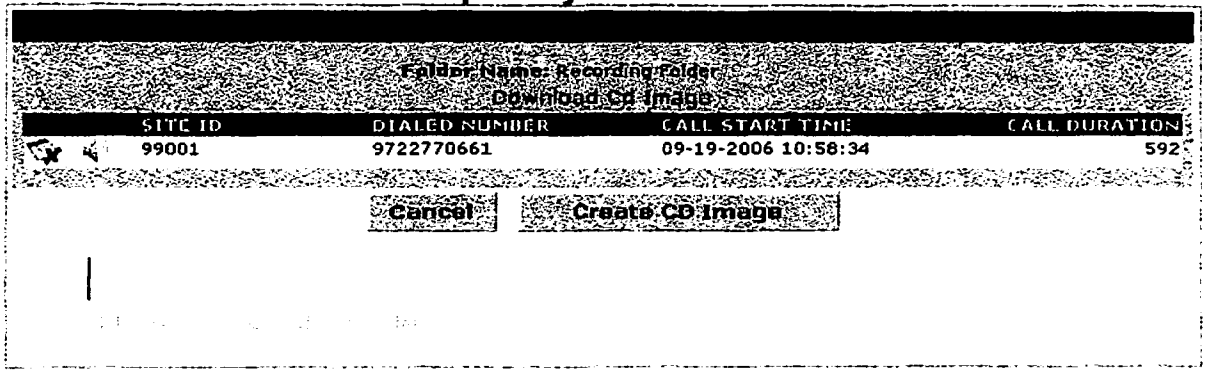
5.13.13 The recording system workstations shall be networked on the WAN described in Section 5.3 so that intelligence analysis and investigation can be performed from other correctional institutions and/or the DOC Central Office. Consideration for speed when downloading a recorded call and the ability to rapidly skip through the call to a specific segment is highly important to the investigative staff. Describe how this can be accomplished with the equipment and software proposed.

☑ **SECURUS has read and will comply.**

Security procedures that allow administrative access to the system at each facility are provided by a multi-level user encrypted password system that requires a known login ID and password before access is granted. A continuous historical audit trail is used to police the access and flow of data and information to and from the computer system. This audit trail records a user ID code and change date with each administrative modification. User groups may be created and maintained by the security administrator. The system also allows a configurable number of attempts to enter a user's ID and password that if exceeded, no further access is permitted until the user ID account is reactivated by the security administrator. All administrative modifications are logged to provide permanent change records.

The Secure Call Platform is equipped with a media player that includes a fast forward function to allow investigators to rapidly skip through the call to s specific segment. A graphic of the media player functions is shown below.

Proprietary and Confidential



5.13.14 The recorded telephone conversations of inmates are sometimes used as evidence in criminal or DOC administrative investigations. Therefore, the recording system proposed with the ITS shall provide a portable laptop computer and a USB portable memory device, to be used as a portable playback system allowing for recorded media to be reviewed on-site at DOC institutions or at required off-site locations. A portable laptop computer shall be provided for each DOC institution listed in Table One of this RFP. Such system shall meet the rules of evidence (e.g. an original digitally recorded medium, date and time-stamped, that if tampered with, would show evidence of such tampering).

☑ **SECURUS has read and will comply.**

The portable laptop computers SECURUS provides are Dell Latitude D520 (Intel Celeron M 520 1.60GHz 533Mhz Single Core, 80GB HDD, 512MB RAM). For more information please refer to *Attachment C – Equipment Specifications.*

5.13.15 The portable playback system shall provide for search capabilities allowing DOC investigators to quickly access certain time periods, certain telephone instruments, etc. The ability to fast forward to a specific time within the recorded call is

of particular importance. The Proposal shall describe how such a system would be provided to DOC and the capabilities and benefits of such a system.

☑ **SECURUS has read and will comply.**

Inmate Telephone System Generated Reports: At a minimum, the ITS will allow the Alaska DOC to generate the required "canned" reports directly through an interface accessible through a secure internet site or via dedicated monitoring terminals. SECURUS will provide reporting capability on all information contained in the inmate telephone system database, including recording of telephone calls. To ensure that reports are accurate and timely, the database will be updated in real time so that all report data is current when viewed and/or downloaded by authorized Department personnel. The database will be capable of maintaining a record of all reports that are downloaded, with the date and time of the download, and the name of the person who performed the download. All reports will have the capability of being queried, sorted or filtered by any field contained in the report or by data parameters, as applicable, and reports shall be readable on screen, printable and will be downloadable into an excel format. Reports will also be viewable via a user-friendly interface. This interface will be, at a minimum a Graphical User Interface (GUI) such as Windows XP. Report formats shall be subject to final approval by the Local Contract Coordinator - Operations or designee.

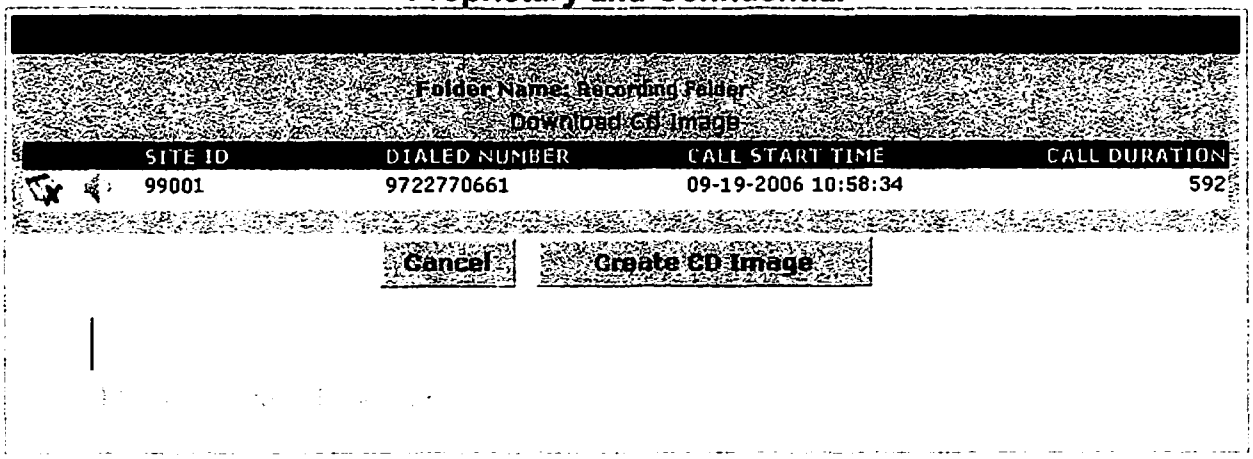
The calling platform is also equipped with a powerful search engine that enables authorized facility personnel access to valuable call detail information and statistical data. This application provides standard reports with parameter fields that allow the user to define the information content of each report based on the following criteria options:

- **Per Originating phone location**
- **Inmate PIN Number**
- **Destination number (partial and/or full number entry)**
- **Date and time range**
- **Call duration and call frequency**
- **Call type (i.e. completed, incomplete, blocked, etc.)**
- **Number restriction and/or status assignment**
- **Personal allowed number cross referencing**
- **Graphical display of call fluctuation**
- **Local, intraLATA, interLATA, interstate and international**
- **Broad search with no data entry**
- **Suspected fraudulent call activity**

The Investigative Reports compiles the data and displays the information on the workstation monitor in report format 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 no limits to the type of information available through the Investigative Reports. This unique application will even assist you in generating a report with little or no concrete information available. For example, our Frequently Called Number Report will display information relative to the amount of calls to a particular number and reflect the location(s) from within the facility the number was called.

In addition to the above, the Agency can take advantage of the ITS' ability to provide customizable reports specific to the Alaska DOC.

The Secure Call Platform is equipped with a media player that includes a fast forward function to allow investigators to rapidly skip through the call to s specific segment. A graphic of the media player functions is shown below.



5.13.16 The PIN shall be recorded at the beginning of each conversation.

☑ **SECURUS has read and will comply.**

5.13.17 The recording equipment shall have "hot swappable" drives and power supplies.

☑ **SECURUS has read and will comply.**

5.14
General ITS Operational Requirements

5.14.1 The Proposal shall describe how the proposed ITS will operate as follows:

A. Within each DOC facility;

☑ **SECURUS has read and will comply.**

Each site processes calls independently, allowing flexibility for design at each site; however all data resides centrally, so authorized users can access functions from any PC with an Internet connection.

B. Throughout all DOC facilities/systems; and

☑ **SECURUS has read and will comply.**

All records can be accessed from any Alaska DOC facility, with appropriate authorizations in place.

B. In conjunction with the Offeror's organization/facilities.

☑ **SECURUS has read and will comply.**

Remote diagnostics, analysis, and monitoring of the Secure Call Network (SCN) are performed by Sentinel. Sentinel is SECURUS' system and networking monitoring package that proactively alerts technical personnel of irregularities in the system software and hardware. The system maintains connectivity to the SCN over the Wide Area Network (WAN). Sentinel continually monitors key trouble areas and automatically assigns service consultants and/or dispatches field technicians to insure optimal operation of your system 24/7. Sentinel actively monitors communication channels, CPUs, disks, messages, processors and servers to insure optimal operations at all times.

Sentinel is available from the SECURUS secure MPLS network and authorized Alaska DOC personnel will receive an access link. Each indicator is polled once every five minutes to determine its status.

5.14.2 The Proposal shall describe the network of services required to support the proposed ITS (i.e., ISDN, T-I, and frame relay.). The new network must not be a part of any public network.

☑ **SECURUS has read and will comply.**

All Calling Platforms provided by SECURUS interface with industry standard Analog and Digital provisioned circuits such as POTS, ISDN, PRI, T-1/DS-1 and DS-3 services. The trunks to be provisioned for the Alaska DOC will be Primary Rate Interface (PRI) T-1's known by the industry as smart trunks. The PRI's provide detailed information for advanced call routing, call progress and enforce outgoing service only. The new network proposed by SECURUS is not part of any public network.

5.14.3 The Proposal shall describe how remote access to the ITS system shall be provided.

☑ **SECURUS has read and will comply.**

Each remote site can be connected to a central site using SECURUS-provided bandwidth. This connectivity provides a data link from the remote platforms to the central site for transferring call records and user profiles. Call records are generated centrally and reports and data can be retrieved from remote sites. New or updated user profiles and system configuration data are managed centrally through the Secure Call Platform and can be updated by authorized users at any site. Authorized users from any site have the ability to login to operate the system, change system configuration, troubleshoot, and retrieve data. The system security features at both the central site and each remote site strictly control this operation. System operators must have a security clearance based on passwords, user –IDs, and security levels to gain access to any individual features of the proposed ITS.

Each call control platform is comprised of three main functions: the Telephony Interface, a Validation Service, and a Graphical User Interface (GUI) system administration application.

5.14.4 The Proposal shall describe all electrical and environmental requirements of the ITS system for each DOC facility. Such information shall be provided for all components of the ITS including central processor, recording and monitoring equipment, etc.

☑ **SECURUS has read and will comply.**

Each system requires a minimum area of two (2) feet wide by three (3) feet deep by four (4) feet high, in a temperature and humidity controlled environment. At least one, preferably two, isolated 120V/20A electrical circuit is required. Each administrative workstation requires minimal desk space or the same space as a personal PC with monitor, PC Speakers, keyboard, printer and mouse.

Temperature/Environment

Operating Temperature	**0° C to 60° C**
Storage Temperature	**-40° C to 70° C**
Humidity condensing	**5% to 90% non-condensing**

5.14.5 The Offeror shall provide and install adequate surge protection for the proposed ITS and its components. The use of traditional "power strips" for surge is not acceptable for this requirement.

☑ **SECURUS has read and will comply.**

All UPS equipment provides electrical surge, lightning and power conditioning protection as well. The system is a fully electronic-based switching system and will include a backup power supply; in the event the centralized processor fails, the uninterruptible power supply (UPS) backup will maintain the system and allow calls to be completed. The system has a sufficient UPS system installed to ensure complete uninterrupted operation of the system, including recording and network services, for a minimum of one hour.

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

5.14.6 The Offeror shall provide and install adequate lightning protection equipment on all network services supplied for the proposed ITS.

☑ **SECURUS has read and will comply.**

All UPS equipment provides electrical surge, lightning and power conditioning protection as well. The system is a fully electronic-based switching system and will include a backup power supply; in the event the centralized processor fails, the uninterruptible power supply (UPS) backup will maintain the system and allow calls to be completed. The system has a sufficient UPS system installed to ensure complete uninterrupted operation of the system, including recording and network services, for a minimum of one hour.

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

5.14.7 The Offeror shall provide an adequate number of uninterruptible power supply (UPS) systems that also have surge protection and line conditioning at each DOC facility capable of supporting all ITS components, including call processors and recording and monitoring devices for a minimum of 1 hour. A UPS capable of supporting each workstation/printer for a minimum of 15 minutes shall also be included.

☑ **SECURUS has read and will comply.**

The system has a sufficient UPS system installed to ensure complete uninterrupted operation of the system, including recording and network services, for a minimum of one hour. All UPS equipment provides electrical surge, lightning and power conditioning protection as well. The system is a fully electronic-based switching system and will include a backup power supply; in the event the centralized processor fails, the uninterruptible power supply (UPS) backup will maintain the system and allow calls to be completed..

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

5.14.8 The Offeror shall provide, install and maintain all ITS UPS system equipment at each of DOC facilities. The Offeror shall replace all UPS system equipment upon expiration of the manufacturer's life cycle of the installed product.

☑ **SECURUS has read and will comply.**

5.14.9 The Proposal shall describe what will occur when commercial power to the ITS is lost.

☑ **SECURUS has read and will comply.**

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

5.14.10 In the case of the loss of commercial power and the failure of the UPS system, the ITS must automatically restrict or "shut off' all Inmate Station Equipment (Telephones) so that no inmate calls can be made until commercial power is restored.

☑ **SECURUS has read and will comply.**

If commercial power is not restored prior to the exhaustion of UPS power, the system will terminate all calls in progress and shut down.

5.14.11 The Offeror shall propose an ITS capable of recovering from a power outage automatically or remotely, once commercial power is restored.

☑ **SECURUS has read and will comply.**

The system will fully recover from any power failure automatically, within five (5) minutes, with no outside intervention required.

5.14.12 The Proposal shall describe the space requirements associated with the ITS equipment and software. The Proposal shall clearly define how much physical space is required for each hardware component. The Offeror should be aware that limited space is available in DOC facilities and that a smaller rather than larger space requirement is desired.

☑ **SECURUS has read and will comply.**

All SECURUS equipment is housed in either 7' Standard Telco Relay rack or in a 4' wheeled rack in a standard 19" mounting width. Each requires 1 standard footprint of 2' X 3' and adequate backboard space to secure 66 blocks and cabling. Usually 4' x 4' is enough space. Site requirements will vary. Components may vary by application but may include Integrated Access Devices (IADs) for TDM to VOIP conversion and control, UPS systems, and switching gear at a minimum as well as a server with storage.

Only one rack will be required per site.

5.14.13 The proposed ITS call processor and recording equipment application software shall be administered and operated from a single workstation. The Proposal shall describe such workstation and how the respective manufacturers will remotely maintain application software without compromising other application software and data.

☑ **SECURUS has read and will comply.**

The SECURUS Secure Call Platform (SCP) is a Netcentric system riding a private network connection using Multi Protocol Label Switching T-1's directly connected to the SECURUS Central Office. Our offer includes dedicated workstations connected to our network as determined by the State of Alaska; however these workstations are not required for anywhere/anytime access nor do they include proprietary software for access to user utilities. Authorized Department Personnel can access all features, including administrative and investigative tools from the central database, through a Secure Socket Layer (SSL) Website from any Windows based PC with access to the World Wide Web. The need for dedicated workstations or interfacing directly with the facilities LAN is not required.

The architecture of Secure Call Platform is built to maintain application software and implement upgrades in real time limiting disruption to the phone service. As new features are Generally Available (GA), the feature is added to the central processor making the feature available to all facilities but will not be turned on unless the Alaska DOC authorizes SECURUS to do so If service has to be disrupted for maintenance or an upgrade, the scheduled work will be conducted between the hours of 1 am - 4 am, and usually never for more than 5 minutes.

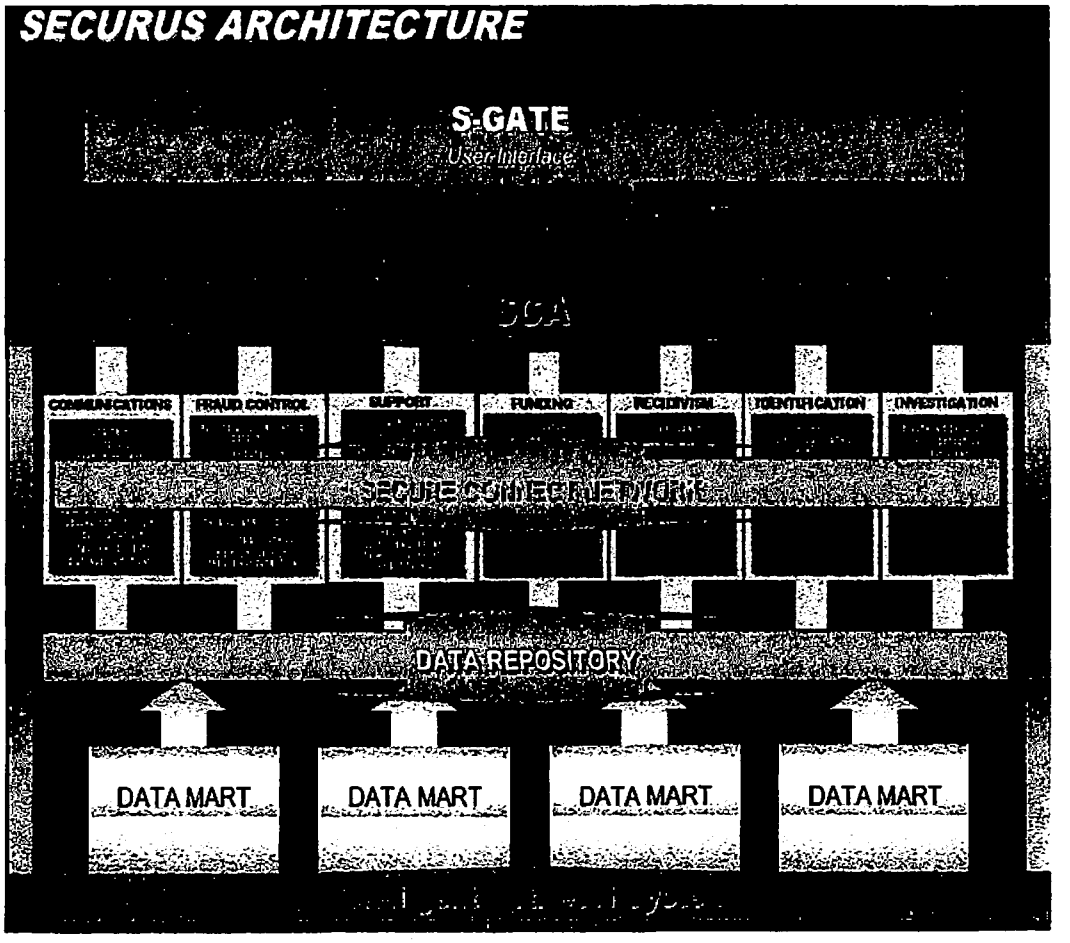
5.14.14 The workstations(s) shall utilize Windows XPB client operating system software or other system approved by DOC. The operating system software shall provide a Graphical User Interface (GUI). Offerors should provide a complete description of any system offered."

☑ **SECURUS has read and will comply.**

The SECURUS Secure Call Platform uses a unique transport architecture that allows us to service sites by private data network, public internet, or traditional telephony. This unique transport allows us to serve sites with thousands of phones or sites with a single phone using the same set of features and allowing all calls to be accessible in a single data view.

SECURUS' Secure Call Platform includes S-Gate, a single entry web portal Graphical User Interface (GUI) for correctional facilities and friends and families of the inmates.

S-Gate along with SECURUS' Secure Connect Architecture provides the foundation of a future array of software applications that will include video, voice, data, biometric and other capabilities.



SECURUS' S-Gate Portal opens a secure window into a facility's operations, providing authorized personnel with the access to an array of functions and modules that are designed to aid correctional facility in maintaining safe and efficient operations. Whether your staff needs to investigate inmates' potentially fraudulent activities, require technical support, or want to inquire as to the status of a commission check, the information is at your fingertips and available 24 hours a day, 365 days a year.

Advantages of Secure Connect Network™

SECURUS' Secure Connect Network™ (SCN) is unlike any communications network in the industry. SCN is the only calling platform built entirely on a net centric, digital transmitted system which produces a "clean" transmission flow for all calls. With SECURUS' web-based technology, all features of the calling system, including recording and monitoring, can be accessed remotely through any PC with internet access.

Complete Flexibility

The SECURUS Secure Call Platform's centralized capabilities allow facility personnel complete control over most system features from any computer. User friendly functionally allows facility staff to turn on a pod, restrict a phone, change a language, turn on or off a feature or application. All this and more can be easily accomplished with the click of a button. Your system will have the flexibility to conform to all of your facilities operations and requirements, not requiring you to conform to an inflexible system.

Immediate Upgrades

The centralized Secure Call Platform also allows for immediate Alaska DOC-wide system upgrades and repairs from one central location, eliminating the need to wait for a field technician to access your system on-site. The ease of upgrading your system enables us to assure the Alaska DOC that they will always be equipped with the latest technology and never utilize an obsolete system.

Data Security

With SECURUS' centralized Secure Call Platform, all facility data is replicated on regionalized, fully redundant data repositories for easy secured retrieval, from any location, by any MDOC authorized user's only. If there is an MPLS outage or a call processing outage, the user will still have access to calling data for inquiry and investigation purposes. Access issues and loss of data due to hard drive or other system failures, are a thing of the past. The platform's fully redundant system is placed in a Class IV disaster resistant data center to assure data integrity.

Pro-Active Monitoring

The centralized Secure Call Platform allows SECURUS personnel to remotely monitor not only hardware issues but also to pro-actively monitor call flow activity, data transmissions and specific phone activity, to assure your system is running at peak performance.

5.14.15 Each work site shall have multiple port 100-Base-T connections. The Proposal shall describe what is necessary to accomplish such a connection.

☑ **SECURUS has read and will comply.**

SECURUS will provide 100BaseT through the use of 10/100 switches.

5.14.16 The Offeror shall provide matching manufactured "Equipment Racks" for call processors and recording and monitoring equipment. System hardware accessories shall also be rack mounted. The Proposal shall provide manufacturers' cut sheets and face layouts.

☑ **SECURUS has read and will comply.**

Manufacturers' cut sheets and face layouts for SECURUS' racks are included in *Attachment D – Manufacturer's Cut Sheets (Racks).*

5.14.17 The proposed call processing and recording equipment shall be remotely located in a telephone or computer room or other location to be designated by DOC. The Proposal shall explain how this remote location shall be accomplished and provide line diagrams showing how equipment will be connected.

☑ **SECURUS has read and will comply.**

Our centralized solution provides an advanced method of aggregating data and providing centralized management of a large system with many remote satellite sites. Each remote site is connected to a central site using MPLS (Multi Protocol Label Switching) T-1's for voice and data providing centralized management of user profiles. New or updated user profiles and system configuration data are archived at the central site for centralized management. Remote users have the ability to login to the centralized site when necessary to operate the system, change system configuration, troubleshoot, and retrieve data. The system security features at the central site strictly control this operation. System operators must have a security clearance based on passwords, user-IDs, and security levels to gain access to any individual features of the system. All changes to configuration are tracked based upon user profiles and managed through levels of security access.

Line diagrams are provided in *Attachment E – Line Diagrams.*

5.14.18 The Offeror shall provide, at a minimum, a 17"-monitor with each workstation. The Proposal shall indicate the manufacturer and model number of the proposed monitors.

☑ **SECURUS has read and will comply.**

The proposed monitor is a Dell E177FP 17".

5.14.19 Access to administrative functions and data shall be password protected.

☑ **SECURUS has read and will comply.**

SECURUS will provide multi-level password security protection.

The secure access tool is a multi-level password scheme specifically designed to allow facility administrators the ability to assign different levels of access to individuals who will use different features of the system. While a high access level allows clearance to all functions of a particular tool, a medium access level may only allow access to a particular function or functions within the same tool. A low access level may be given to duty officers to routinely use the information search function of a given tool, while denying access or clearance to other functions or features. Each user is tracked by password in an audit trail from the time of logging on to the system.

5.14.20 The workstations shall have a microprocessor of 3 GHz or faster, 1 GB random access memory (RAM), a CD RW drive and a USB portable memory device with enough memory to transport a minimum of 45 calls.

☑ **SECURUS has read and will comply.**

5.14.21 The Offeror shall provide one workstation, printer and one laptop computer at each DOC institution listed in Table One.

☑ **SECURUS has read and will comply.**

5.15
ITS System Capacities

The Proposal shall describe the capacities/limits for the proposed ITS. At a minimum, the Offeror shall provide the capacity for each of the following items:

A. Individual inmate accounts;

☑ **SECURUS has read and will comply.**

The capacity for individual inmate accounts is virtually unlimited.

B. Call records;

☑ **SECURUS has read and will comply.**

The capacity for call records is virtually unlimited.

C. Simultaneous administrative users;

☑ **SECURUS has read and will comply.**

The capacity for simultaneous administrative users is virtually unlimited.

D. Workstations;

☑ **SECURUS has read and will comply.**

The capacity for workstations is virtually unlimited.

E. Silent monitors;

☑ **SECURUS has read and will comply.**

The capacity for silent monitors is virtually unlimited.

F. Simultaneous users of silent monitor equipment;

☑ **SECURUS has read and will comply.**

The capacity for users of silent monitor equipment is virtually unlimited.

G. Inmate telephones; and

☑ **SECURUS has read and will comply.**

The capacity of telephones and telephone calls will be determined by the size of facility and amount of calls generated. There are no limits to the amount of telephone sets but generally the quantity is driven by the demand. The ratio of "inmates to telephones" is usually between "10 and 20 to 1".

H. Telephone calls.

☑ **SECURUS has read and will comply.**

The capacity of telephone calls is virtually unlimited.

5.16
Software Enhancements/Upgrades

5.16.1 The Proposal shall explain the process for handling requests from DOC for ITS software enhancements. Enhancements shall be at no charge to DOC.

☑ **SECURUS has read and will comply.**

With Secure Call Platform, upgrades are automatically downloaded to the system through our secure network each time they are available. Software requests will be handled by the Alaska DOC's Account Manager and will be provided if the requested enhancement can be integrated into the system.

5.16.2 Except for enhancements requested by DOC, the Offeror shall provide, at no cost to DOC, software enhancements/upgrades to the proposed ITS when the enhancement/upgrades are beneficial to either party for the purpose of system

security or operational efficiency. **The installed ITS shall always have the latest general release of the system software including operating systems for the system administration or system reporting terminals/PCs.** Beta and field-tested software shall not be provided unless specifically approved by DOC. Prior to any software upgrades or enhancements, the Offeror shall discuss the software benefits with DOC and proceed only after DOC written approval by the contracting officer. A computer system review for upgrade/update will be required at the end of the second year of the Contract.

☑ **SECURUS has read and will comply.**

5.17
General ITS Management Requirements

5.17.1 The Offeror shall propose an ITS that can be administered on-site by Offeror or DOC personnel.

☑ **SECURUS has read and will comply.**

5.17.2 The Offeror shall propose an ITS that allows for changes to be administered in "real time" while the system is in use. The proposed system shall not require the system to be taken off-line to make additions, changes or retrieve reports.

☑ **SECURUS has read and will comply.**

5.17.3 The Proposal shall describe what system administration functions are available with the proposed ITS (i.e., new account entry, account/record modification and account deletion). The Proposal shall provide samples of its user interface screens.

☑ **SECURUS has read and will comply.**

At any time, day or night, authorized Alaska DOC personnel can use SECURUS' S-GATE™ Portal system administrator functions. S-Gate provides a secure window into the facilities operations. Users can securely access all calling activity, including all call detail reports. The customized user interface allows approved users to check and track facility commission data and review monthly commission payments. In addition, facilities can also use the Portal to open new service tickets and view the status of existing service tickets. Document sharing between the facility and our support personnel, is also done through the Portal.

The Portal provides access to call details. You can choose the date range, the site (if you have more than one), the originating number (or all), and the called number (or all). The first report shows you the number of calls and the revenue for that originating number. You can click on the originating number to see more detail: date, time, number of minutes, and revenue for that call. You can even click on the called number to see who that number is registered to (if it's listed).

The Portal shows you commission data for whatever date range you specify. The previous three months always show, and you can select other months by entering appropriate dates. For each month, you see the total number of calls, the total minutes, the overall revenue, and your facility's commission.

Samples of SECURUS' user interface screens are provided in *Attachment F – SECURUS User Interface Screens*. Please note these screen shots are proprietary and confidential.

5.17.4 The Proposal shall describe the transfer of inmate records when an inmate is moved from one DOC facility to another.

☑ **SECURUS has read and will comply.**

Inmate records will be kept on a shared database, with all of the Alaska DOC facilities having access. Therefore, inmate transfers between department facilities will not require any records transfer.

5.17.5 The Proposal shall describe the ITS system security for all data stored locally or in a central database. Such security description shall include system security as well as how access to such sensitive information shall be performed within the Offeror's organization.

☑ **SECURUS has read and will comply.**

Data Integrity
Facilities no longer have to fear losing data because of local disasters such as hurricanes, floods, fires, localized security breaches or lightning. All facility data is replicated on regionalized, fully redundant data repositories for easy secured retrieval, from any location, by any Alaska DOC authorized user's only. If there is an MPLS outage or a call processing outage, the user will still have access to calling data for inquiry and investigation purposes, Access issues and loss of data due to hard drive or other system failures, are a thing of the past. The platform's fully redundant system is placed in a Class IV disaster resistant data center to assure data integrity.

Pro-Active Flexibility
Secure Call Platform allows SECURUS personnel to remotely monitor not only hardware issues but also to pro-actively monitor call flow activity, data transmissions and specific phone activity, to assure your system is running at peak performance.

Network Protection
SECURUS applies a high level of security to protect our customers and ourselves from cyber-pirates. Applications transmitting data across public networks are supporting SSL, CERTS, and 128 bit encryption. Cisco and Juniper firewalls are utilized throughout the network to protect SECURUS and its customers by creating DMZ networks, which result in multiple levels of firewall

protection. In addition, Tipping-Point Intrusion Prevention System (IPS) and Intrusion Detection Systems (IDS) devices are used at our data centers and at the corporate headquarters. All Servers, laptops, workstations require anti-virus & anti-spyware protection software and latest operating systems patches. SECURUS supports both AVG and Symantec anti-virus.

Network and Site Monitoring
The SECURUS network consist of many servers each providing a different business critical application or service. All applications that affect the business are monitored.

Facility Monitoring
Redundant monitoring systems, all with paging capability, are in place, alerting on-site engineers of any system threshold inconsistencies. Redundant page alerts are also sent to the Network Operations Center (NOC) to create a Ticket of the event, which is then sent to the data center via e-mail, page, and phone call, as a redundant notification process.

The onsite infrastructure engineers make scheduled daily inspections of all infrastructure systems and routinely perform preventative maintenance.

Security
The SECURUS centralized data center in Allen, Texas, maintains some of the most comprehensive security measures in the industry. Access to network facilities is controlled through six levels of mandatory physical security and an escort is required in areas that house critical components of our system.

Access by SECURUS Personnel
SECURUS understands the importance of keeping facility data secure. Access to Alaska DOC data will only be provided to personnel working directly on the project.

5.18
Data Back-up

5.18.1 The Proposal shall describe the process for ensuring data integrity both in the local and central databases.

☑ **SECURUS has read and will comply.**

Data Back-ups and Storage
The redundancy built in to the SECURUS system effectively prevent loss of data and system downtime because all of the data is stored in an offsite, centralized database and backed up at multiple locations across the nation. Because the system is web-based, the data can be accessed at any location with an internet connection, and SECURUS' Secure Connect Architecture maintains the system at the highest level of operability.

In addition, all call records will be duplicated and backed-up at two fully-staffed data centers in Allen and Dallas, Texas. Each data center comprises two fully

redundant systems, each with its own circuit feed, its own physical racks, redundant communication, redundant termination carriers, and redundant A&B power with UPS and generator backup. The physical storage itself is also advanced; the data is stored via both SAN and robotic tape, and the data centers are connected to one another by a Metropolitan Area Network Ring. Additionally, the system features full state awareness of each call with the ability to fail over to another data center if necessary, in most cases without dropping the call in progress.

Data Backup/Redundancy

The system is a fully electronic-based switching system and will include a backup power supply; in the event the centralized processor fails, the uninterruptible power supply (UPS) backup will maintain the system and allow calls to be completed. The system has a sufficient UPS system installed to ensure complete uninterrupted operation of the system, including recording and network services, for a minimum of one hour. All UPS equipment provides electrical surge, lightning and power conditioning protection as well.

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

Site and Server Redundancy

The centralized data center is located in Allen, Texas. We provide a secondary data center in Dallas, Texas and a Disaster Recovery data center in Irving, Texas. These three data centers provide SECURUS with both site-level and server-level redundancy. SECURUS recently completed the process of building a regional data center to support the Secure Call Platform infrastructure in Atlanta, Georgia. Additional sites are being reviewed if the need arises.

Each remote site can be connected to a central site using SECURUS-provided bandwidth. This connectivity provides a data link from the remote platforms to the central site for transferring call records and user profiles. Call records are generated centrally and reports and data can be retrieved from remote sites. New or updated user profiles and system configuration data are managed centrally through the Secure Call Platform and can be updated by authorized users at any site. Authorized users from any sites have the ability to login to operate the system, change system configuration, troubleshoot, and retrieve data. The system security features at both the central site and each remote site strictly control this operation. System operators must have a security clearance based on passwords, user –IDs, and security levels to gain access to any individual features of the proposed ITS.

Component Redundancy
With the SECURUS system, the chance of total system failure is essentially eliminated because in the event that any one component fails, the system will automatically switch to another, properly functioning component – in most cases with no disruption to service. The system enhancements that allow for such comprehensive reliability are listed below:

- **Every 24 phones or less get own IAD**
- **Phones diverse wired with multiple IAD**
- **Each IAD has diverse T1s**
- **T1s use MPLS to primary & backup data centers**
- **Unique wiring scheme with separate hardware**
- **Centralized system using carrier class components to minimize downtime**
- **Use of public internet connection for connectivity in case of failure in point-to-point connection**

5.18.2 The Offeror shall perform all system and database back-ups and archiving. The Offeror shall provide all archival hardware, supplies, and network and recovery procedures to ensure that no data will be lost.

☑ **SECURUS has read and will comply.**

5.18.3 The Offeror shall be capable of recovering all ITS system data for all locations, to the point of full system operation, using a system backup.

☑ **SECURUS has read and will comply.**

5.18.4 The Proposal shall describe the back-up schedule for the following:

A. The local databases for each DOC facility; and

☑ **SECURUS has read and will comply.**

All databases are centrally located with multiple levels of redundancy. The failsafe built in to the SECURUS system effectively prevent loss of data and system downtime because all of the data is stored in an offsite, centralized database and backed up at multiple locations across the nation. Because the system is web-based, the data can be accessed at any location with an internet connection, and SECURUS' Secure Connect Architecture maintains the system at the highest level of operability.

In addition, all call records will be duplicated and backed-up at two fully-staffed data centers in Allen and Dallas, TX. Each data center comprises two fully redundant systems, each with its own circuit feed, its own physical racks, redundant communication, redundant termination carriers, and

redundant A&B power with UPS and generator backup. The physical storage itself is also advanced; the data is stored via both SAN and robotic tape, and the data centers are connected to one another by a Metropolitan Area Network Ring. Additionally, the system features full state awareness of each call with the ability to fail over to another data center if necessary, in most cases without dropping the call in progress.

B. The central database for the entire ITS system.

☑ **SECURUS has read and will comply.**

All databases are centrally located with multiple levels of redundancy. The databases are instantaneously and continuously backed up through the use of SAN. Call detail records will be stored online according to the terms set forth by the Alaska DOC, after which time, they are backed up to tape.

The failsafe built in to the SECURUS system effectively prevent loss of data and system downtime because all of the data is stored in an offsite, centralized database and backed up at multiple locations across the nation. Because the system is web-based, the data can be accessed at any location with an internet connection, and SECURUS' Secure Connect Architecture maintains the system at the highest level of operability.

In addition, all call records will be duplicated and backed-up at two fully-staffed data centers in Allen and Dallas, Texas. Each data center comprises two fully redundant systems, each with its own circuit feed, its own physical racks, redundant communication, redundant termination carriers, and redundant A&B power with UPS and generator backup. The physical storage itself is also advanced; the data is stored via both SAN and robotic tape, and the data centers are connected to one another by a Metropolitan Area Network Ring. Additionally, the system features full state awareness of each call with the ability to fail over to another data center if necessary, in most cases without dropping the call in progress.

5.18.5 The Offeror shall provide for all database information to be stored off site from the Offeror's location (see Section 5.3.04). The Proposal shall describe how this "copy" will be kept current with the other system backups.

☑ **SECURUS has read and will comply.**

In addition to the network redundancy, onsite redundancy will occur across MPLS circuits at each site, retaining all information on 4 terabyte servers with Raid 5 arrays. SECURUS will maintain a frequent backup schedule to ensure the onsite data mirrors the central database.

5.18.6 The Proposal shall acknowledge that DOC owns all archived information, call detail, inmate records, etc.

☑ **SECURUS has read and will comply.**

We agree that the Alaska DOC owns all inmate records and call recordings. It is SECURUS' policy that its systems, applications, and related documentation and detail call records remain our sole and exclusive property which we have the unlimited right to use call detail records, data and information for investigative and law enforcement purposes. However, during the term of the Agreement and for a reasonable period of time thereafter, we will provide you with reasonable access to the call detail records.

5.19
ITS System Reports

5.19.1 The proposed ITS shall provide reporting and querying methods and capabilities that provide maximum flexibility, a user-friendly interface, speed, efficiency and accuracy. The Proposal shall describe the reporting capabilities of the proposed ITS.

☑ **SECURUS has read and will comply.**

The system will be capable of real-time and delayed call record reporting by time of day, date of call; call duration shall frequently called number, PIN number, dialed number, phone, area code, telephone exchange cost of call, or any combination thereof. The system will also be capable of allowing the Alaska DOC to form its own reports based upon the data that the phone system collects.

The SECURUS system's reporting tool can provide routine scheduled reports or reports on an ad hoc basis. The system is capable of searches and call detail analysis on all calls placed from each inmate telephone through the system which includes date, time and duration, telephone number or origination and destination, if utilized, inmate ID, reason for termination, and much more. Call details are kept on all call attempts, except those to blocked numbers.

The standard reports can be customized by varying search criteria such as date range, facility, or call length. These standard reports can be customized to meet the Alaska DOC needs.

The calling platform is equipped with a powerful search engine that enables authorized facility personnel access to valuable call detail information and statistical data. This application provides standard reports with parameter fields that allow the user to define the information content of each report based on the following criteria options:

- **Per Originating phone location**
- **Inmate PIN Number**

- **Destination number (partial and/or full number entry)**
- **Date and time range**
- **Call duration and call frequency**
- **Call type (i.e. completed, incomplete, blocked, etc.)**
- **Number restriction and/or status assignment**
- **Personal allowed number cross referencing**
- **Graphical display of call fluctuation**
- **Local, intraLATA, interLATA, interstate and international**
- **Broad search with no data entry**
- **Suspected fraudulent call activity**

The Investigative Reports feature compiles the data and displays the information on the workstation monitor in report format 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 no limits to the type of information available through the Investigative Reports. This unique application will even assist you in generating a report with little or no concrete information available. For example, our Frequently Called Number Report will display information relative to the amount of calls to a particular number and reflect the location(s) from within the facility the number was called.

In addition to the above, the Alaska DOC can take advantage of the system's ability to provide customizable reports specific to their your requirements.

The SECURUS Web Portal will provide the Alaska DOC with the ability to access, share and review call record detail, and service request status online—anywhere and anytime. This means the Alaska DOC will have the capability to continuously monitor other significant data elements.

5.19.2 The proposed ITS shall allow for the generation of reports by a DOC facility, including Central Office, a combination of DOC facilities or all DOC facilities.

☑ **SECURUS has read and will comply.**

5.19.3 The proposed ITS shall allow for the generation of reports by DOC personnel based on their user level restriction.

☑ **SECURUS has read and will comply.**

5.19.4 The proposed ITS shall allow for the generation of reports by a user-friendly interface. The Proposal shall describe how the user interface will be used for generating reports.

☑ **SECURUS has read and will comply.**

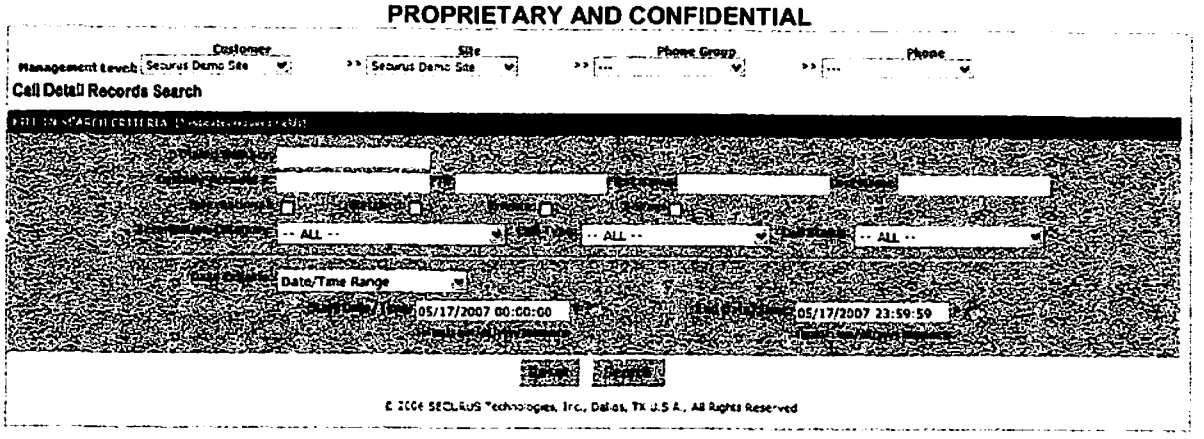
The Secure Call Platform has a dedicated reports writer that provides investigative information based on the Call Detail Records. This sophisticated reporting tool can provide routine scheduled reports, or reports on an ad hoc basis. This means, in almost every case, the Alaska DOC will be able to create your own reports, selecting whichever criteria you need included. These reports are available immediately.

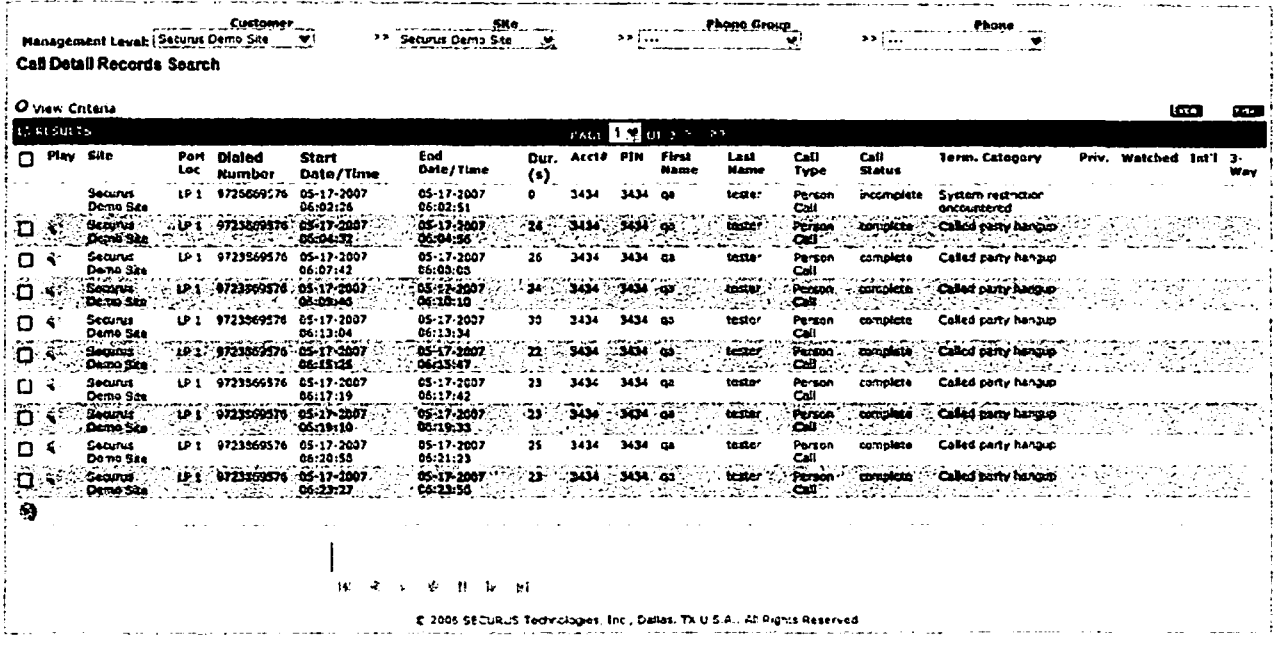
The Secure Call Platform is capable of searches and call detail analysis on all calls placed from each inmate telephone through the system which includes date, time and duration, telephone number or origination and destination, if utilized, inmate ID, reason for termination, and much more. Call details are kept on all call attempts, except those to blocked numbers. The standard reports can be customized by varying search criteria such as date range, facility, or call length.

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

- **Per phone, per location and per inmate**
- **Destination number (partial and/or full number entry)**
- **Date and time range**
- **Call duration and call frequency**
- **Call type (i.e. completed, incomplete, blocked, etc.)**
- **Number restriction and/or status assignment**
- **Personal allowed number cross-referencing**
- **Graphical display of call fluctuation**
- **Local, intralata, interlata, interstate and international**
- **Broad search with no data entry**
- **Suspected fraudulent call activity**

Call detail search parameters and a sample report are shown below.





Investigative Reports

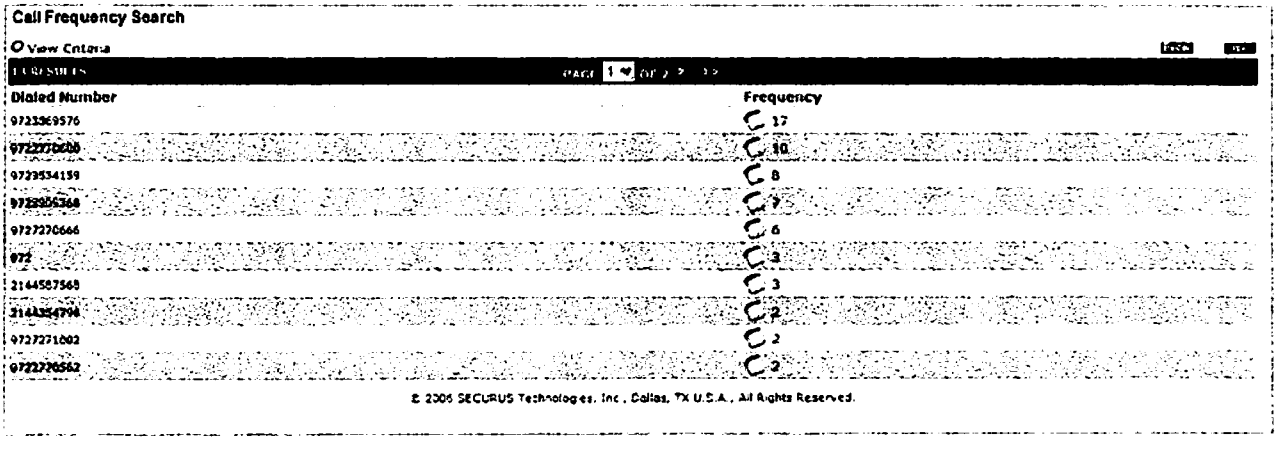
The Investigative Reports application compiles the data and displays the information in a report format, on the workstation monitor, in a matter of seconds regardless of the volume of information retrieved. Further, this application provides multiple functions for call playback, copying calls to remote media and restoring calls from an archival mode. There are no limits to the type of information available through Investigative Reports. This unique application will even assist you in generating a report with little or no concrete information available. For example, our Frequently Called Number Report (FCN) will display information relative to the amount of calls to a particular number and reflect the location(s) from within the facility the number was called.

The FCN feature allows investigators to generate a report by entering a frequency threshold that instructs the system to search for only those numbers that have been called 'x' amount of times throughout the facility. For example,

by entering '50' in the parameter field the system will display only those numbers that have been called 50 or more times within a designated timeframe. Once the report is displayed on screen a simple click of the mouse will automatically produce a second report that represents all areas of the facility from which a specific number has been called. From this report investigators can analyze data to determine specific call patterns, detail suspicious activity and selectively assign a watched number status to potential fraudulent numbers.

A sample *Frequently Called Number Report* is shown below.

PROPRIETARY AND CONFIDENTIAL



Web Portal

The SECURUS Web Portal will provide the Alaska DOC with the ability to access, share and review call record detail, commission information, and service request status online—anywhere and anytime. This means the Alaska DOC will have the capability to continuously monitor and audit commissions and other significant data elements.

SECURUS' Portal opens a secure window into a facility's operations, providing authorized personnel with the access to an array of applications, functions and modules that are design to aid correctional facilities in maintaining safe and efficient operations. Whether you need to investigate inmates' potentially fraudulent activities or require technical support, all functions are available 24 hours a day, 365 days a year.

5.19.5 The Offeror shall provide at least one HP laser printer capable of printing a minimum of 15 pages per minute color printer or equivalent for each institution listed in Table One of this RFP. The Offeror shall provide required maintenance for the Contract term.

☑ **SECURUS has read and will comply.**

5.19.6 The proposed ITS shall allow for the generation of standard system reports as well as reports customized for the specific needs of DOC.

☑ **SECURUS has read and will comply.**

5.19.7 The Proposal shall include samples of its standard system reports.

☑ **SECURUS has read and will comply.**

Sample reports are included in *Attachment G – SECURUS* Sample Reports. SECURUS' screen shots of the sample reports are confidential and proprietary. SECURUS requests that they be held as confidential pursuant to Section 1.13.

5.19.8 The proposed ITS shall allow for selected reports to be generated automatically based on DOC criteria (i.e., time of day, volume of calls and particular inmate). The Proposal shall describe all options available to DOC for this automatic report generation.

☑ **SECURUS has read and will comply.**

SECURUS' Secure Call Platform application allows authorized users to generate reports for printing in either PDF or Excel format. All generated reports can be downloaded to the user's desktop and attached to an email message for delivery as needed.

5.19.9 The proposed ITS shall allow for automatic generation of reports on an DOC facility or system wide basis.

☑ **SECURUS has read and will comply.**

5.19.10 The proposed ITS shall provide adequate processing power and memory to allow for rapid search and report generation capabilities.

☑ **SECURUS has read and will comply.**

5.19.11 The proposed ITS shall allow for all report data to be stored in an ASCII file format on removable electronic storage media (i.e., CD-ROM, high capacity diskette, digital).

☑ **SECURUS has read and will comply.**

5.19.12 The proposed ITS shall allow for all report data to be stored in various electronic formats (i.e., standard DBF, FileMakerB, or Microsoft Excel). The Proposal shall list the available electronic formats.

☑ **SECURUS has read and will comply.**

The SECURUS Correctional WebManage application allows the user to save a report as a file, in the Adobe® PDF format. Reports may be saved to a variety of

destinations. This feature allows for fast and convenient access to reports for future retrieval or sharing.

The reports created by WebManage may be stored in many different formats. Most common file formats are supported. Supported formats include Microsoft Word, Microsoft Excel, Word Perfect, and HTML. The Export feature allows you to use the reports you create in word processors and other office automation tools that you are using today. In addition, reports may easily be published on your facility's web page.

5.19.13 The proposed ITS shall allow for all reports to be viewed in hard copy format or viewed on-line by a user with the proper access level.

☑ **SECURUS has read and will comply.**

5.19.14 The proposed ITS shall provide for the following reports, at a minimum, to be generated for DOC:

A. Chronological List of Calls;

B. Daily Call Volume Summary;

C. Daily Call Volume Detail;

D. Inmate Account Summary;

E. Inmate Account Detail;

F. Frequently Dialed Numbers;

G. Specific Telephone Number Dialed Usage;

H. Suspended Inmate Account:

I. Alert Notification:

J. Telephone Numbers Called by More Than One Inmate;

K. Telephone Numbers Assigned to More Than One Inmate Account;

L. Quantity of Calls per Inmate Account;

M. Quantity of Minutes per Inmate Account;

N. Blocked Telephone Number List;

O. Local Exchange Volume (by Exchange);

P. Area Code Volume (by Area Code);

Q. Hot number list;

R. PIN/destination correlation; and

S. Billed number account information.

☑ **SECURUS has read and will comply.**

5.19.15 The Proposal shall describe if custom queries can be used by DOC on the new central database.

☑ **SECURUS has read and will comply.**

Custom queries can be run on any field or combination of fields in the Secure Call Platform. Additionally, SECURUS will coordinate with the Alaska DOC to create new reports at the DOC's request.

5.19.16 The proposed ITS shall have import capabilities and be interfaced to the administrative PBX so that respective CDR can be merged on a regular basis for the purpose of operational intelligence. Such interface might be accomplished with spare SMDR ports or "Y" cables. Application software shall be provided for generating reports.

☑ **SECURUS has read and will comply.**

In addition to the SCP reporting capabilities, each report can be exported in three main formats; Text, MS Excel and Adobe. SECURUS provides these exportable reports for facilities to use this information for auditing or external system import capabilities. Since SECURUS does not provide services for the Alaska DOC Administrative Private Branch Exchange (PBX) telephone system, we can not commit to its ability of importing these reports into your system. Upon contract award we will work closely with the Alaska DOC in an effort to facilitate this request if deemed necessary.

With the robust reporting modules and anywhere availability of access SECURUS provides with our new Architecture, we are confident that the Alaska DOC will expand their operational intelligence well beyond what is available today.

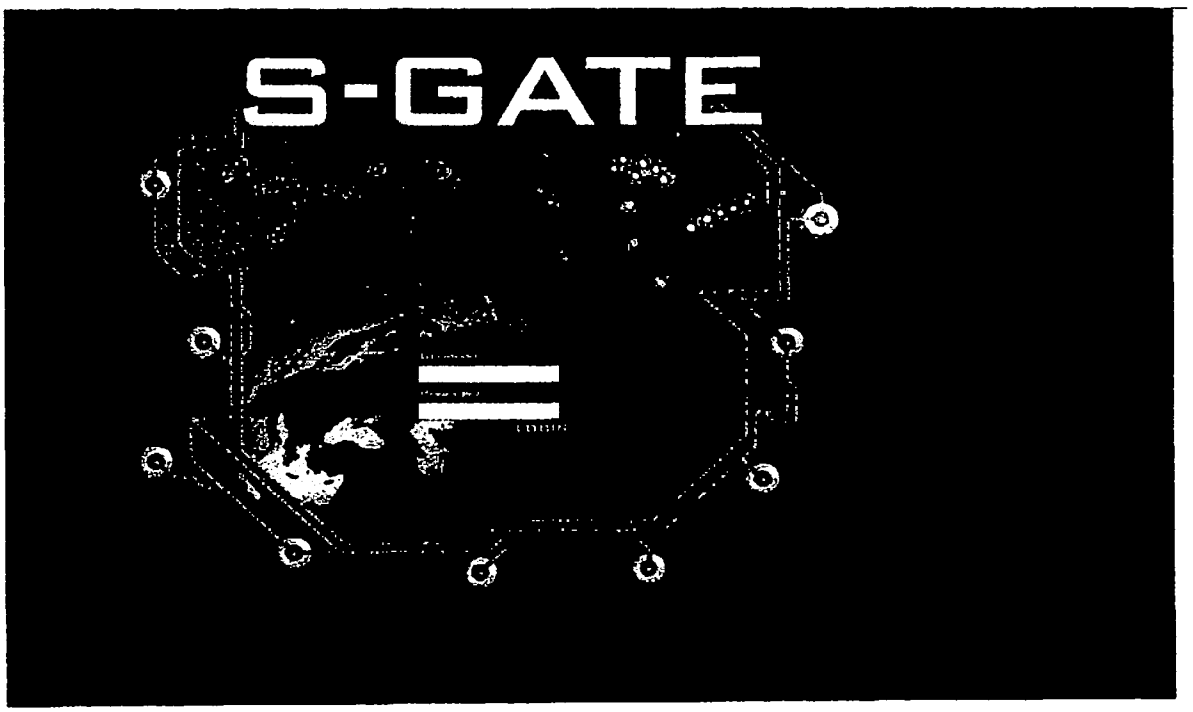
Electronic Dragnet Basic (v2.4)
In order to prevent and solve crime, investigators need accurate and timely intelligence that allows them to quickly and easily gather intelligence about suspicious persons and events. Electronic Dragnet Basic provides investigators a single site with anywhere, anytime access to a wide array of data sources and intelligence tools. Investigators use Electronic Dragnet too quickly and easily access, analyze and save call recordings and other associated information. Investigators are able to use tools that include reverse number lookup, investigator notebook and mapping, in order to develop a *complete inmate profile* that can help to identify links and associations to persons, incidents and activities.

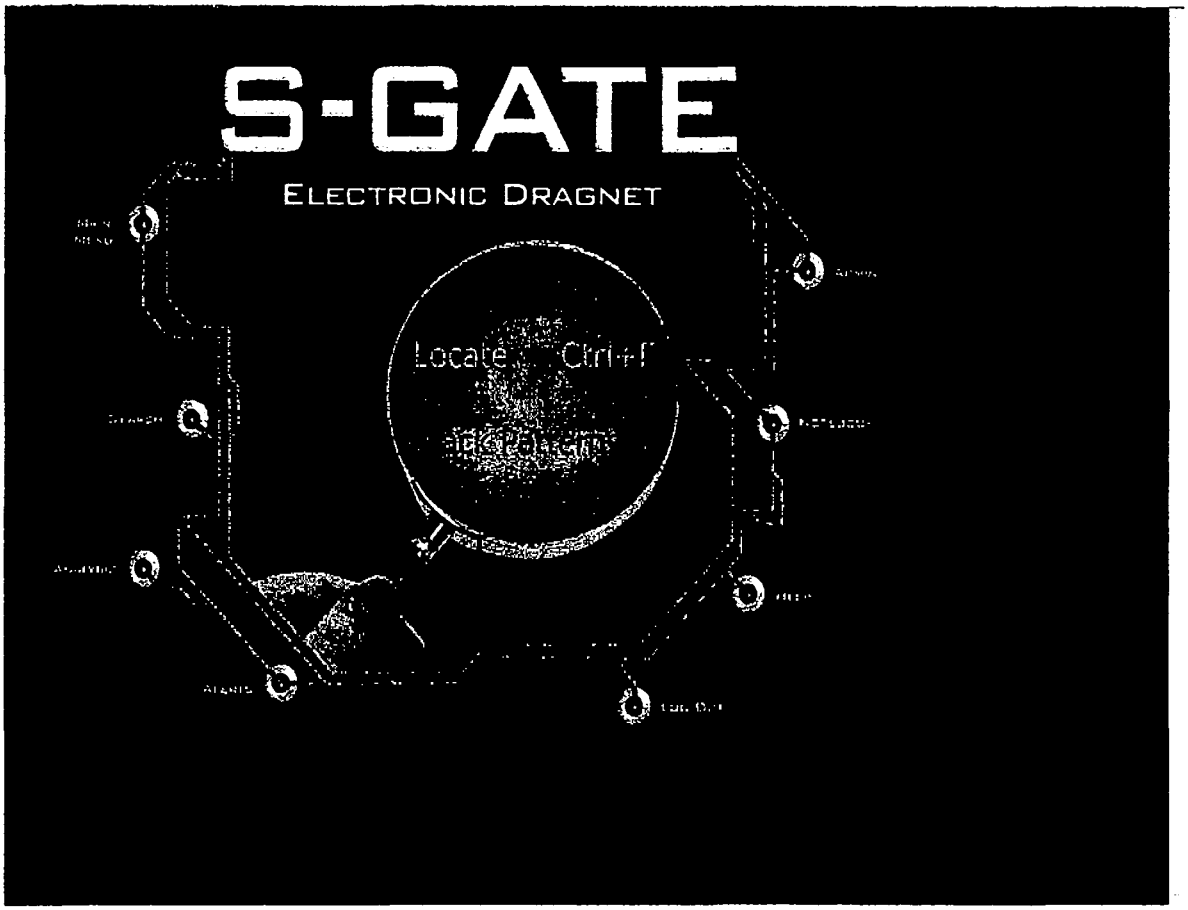
To access Electronic Dragnet Basic v 2.4 a user must have a:

1. **PC with:**
    a. **Internet Explorer 5.0 or greater**
    b. **High speed internet access**

2. S-Gate client license and associated User ID and Password

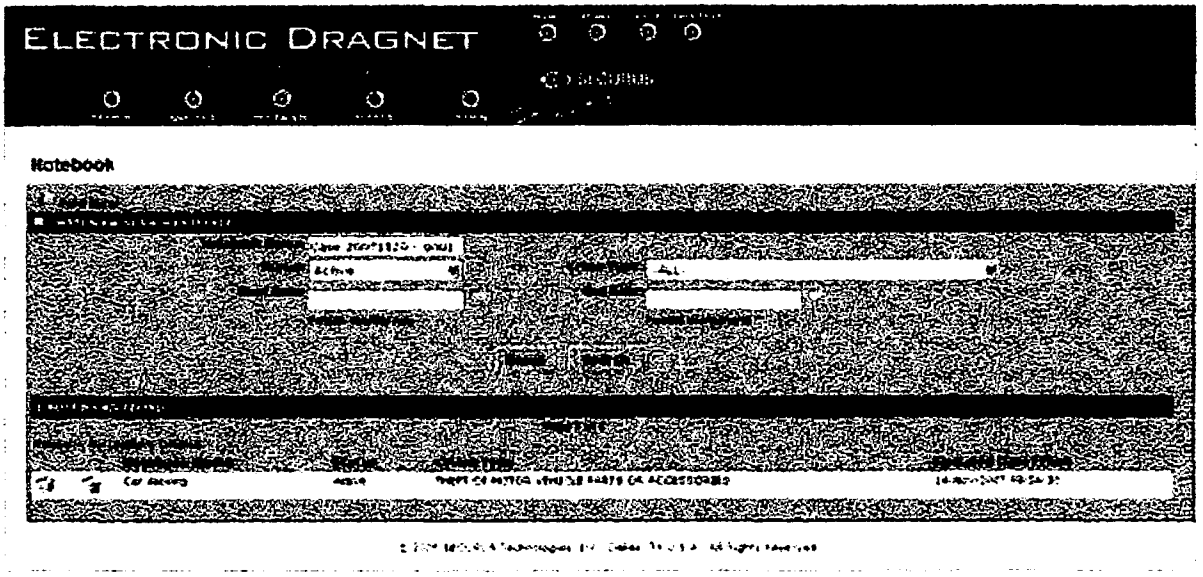
Centralized Single Point of Access
All your investigative activity is accessed from one central location. Our S-GATE user inter-face, provides investigators with the ONLY; easy to use, single point access investigative user interface in the industry. This industry-leading portal, allows investigators any where, any time access to the following data sources and tools.





S-Gate is SECURUS' secure internet portal that allows authorized users to log into both the Secure Call Platform and Electronic Dragnet applications.

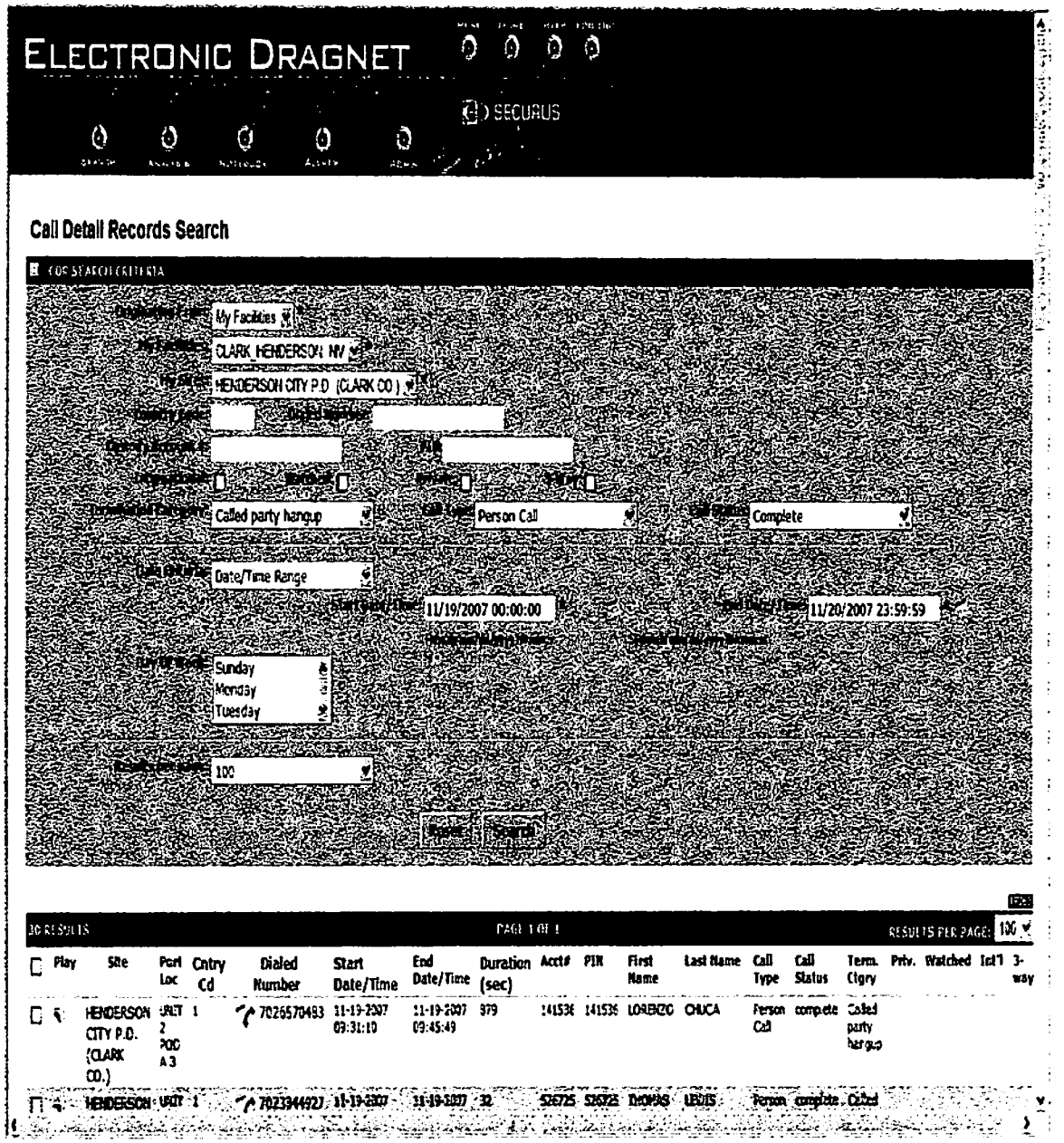
Investigator Notebook
Investigators can create, store and retrieve "case files" in order to store critical case elements (i.e. a call recording or CDR information) that an investigator "discovers" through the use of the Electronic Dragnet investigative tool. The Investigator Notebook is confidential to the assigned investigator. Each investigator can create and store an unlimited number of case files while maintaining the ability to retrieve, view and edit the intelligence through Electronic Dragnet's any time, any where capability.



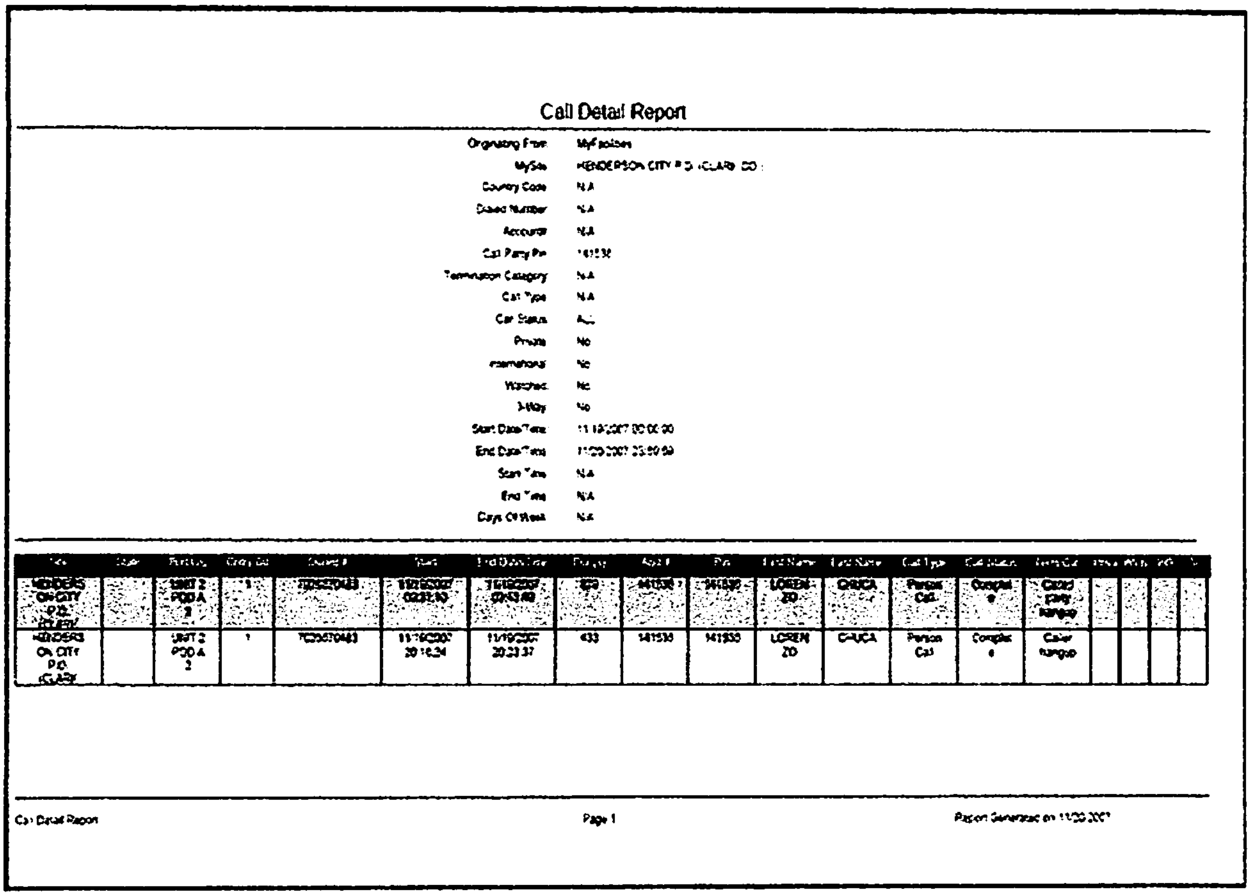
An investigator can use the tools in Electronic Dragnet in a workflow sequence that fits their needs. Many investigators will start an investigation by creating an Investigator Notebook that allows them to create a case file. This confidential file allows the investigator to add notes and save links to recordings and CDR information.

Call Detail Records

Search each call originating from your site or agency. Set specific date criteria such as: date & time range, start date & time, end date & time and day of the week. Check on call status, including any calls attempted, whether completed or incomplete or whether a third party call was attempted. Information is displayed to the screen allowing the investigator to immediately scroll through multiple records and selecting appropriate to: review the actual conversation, save with the Investigator Notebook, conduct a reverse number lookup or display the address on a map. An investigator can turn this display into a PDF report that can be saved and/or printed by clicking on a single button.



An investigator can search a facilities CDR records using a wide variety of criteria. Results are displayed to the screen; the investigator can view the site, dialed number and inmate's name, pin and account information (provided a facility has enabled these features) along with other call detail information.


Call Detail Report

Originating From	MyFacilities
MySite	HENDERSON CITY P.D. (CLARK CO)
Country Code	N/A
Dialed Number	N/A
Account#	N/A
Call Party Pin	141530
Termination Category	N/A
Call Type	N/A
Call Status	ALL
Private	No
International	No
Watched	No
3-Way	No
Start Date/Time	11/19/2007 00:00:00
End Date/Time	11/20/2007 23:59:59
Start Time	N/A
End Time	N/A
Days Of Week	N/A

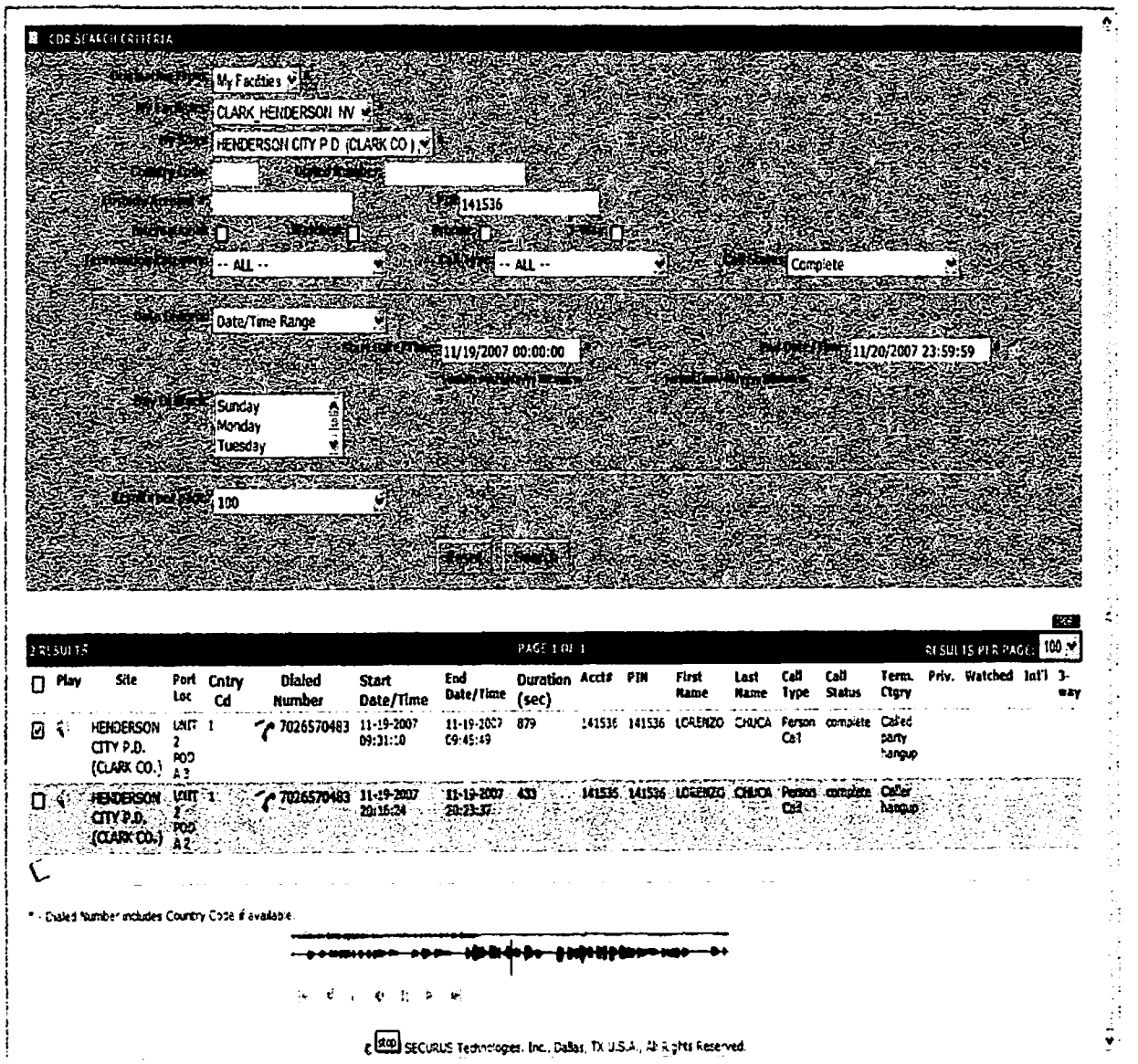
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
HENDERSON CITY P.D. [illegible]		UNIT 2 POD A 2	1	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	LORENZO	CHUCA	Person Call	Complete	Called party hangup				
HENDERSON CITY P.D. (CLARK		UNIT 2 POD A 2	1	7025670483	11/19/2007 20:16:24	11/19/2007 20:23:37	433	141530	141530	LORENZO	CHUCA	Person Call	Complete	Caller hangup				

Call Detail Report Page 1 Report Generated on 11/20/2007

By clicking on the PDF button an investigator can get all the results in a PDF report that can be saved and printed.

Call Recordings

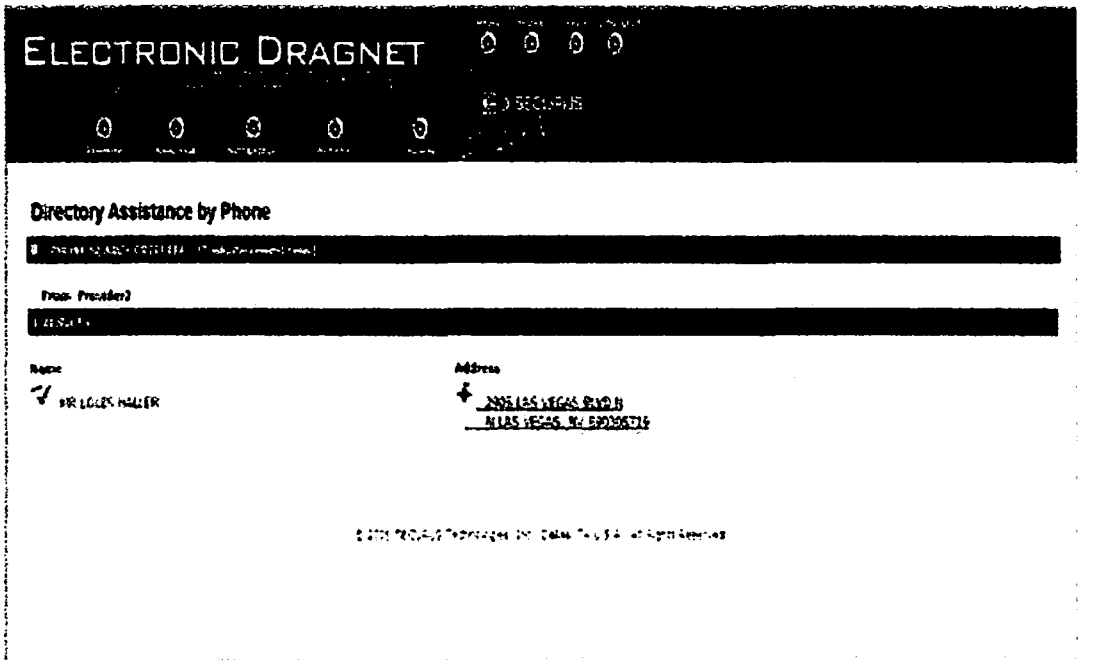
Listen to call recordings through a secure internet browser. SECURUS' digital call clarity and centralized hosted applications allows the investigator access to this critical intelligence resource in the office, in the field (locally or nationwide) or even at home.



An investigator can listen to a call simply by selecting the call and hitting the play button.

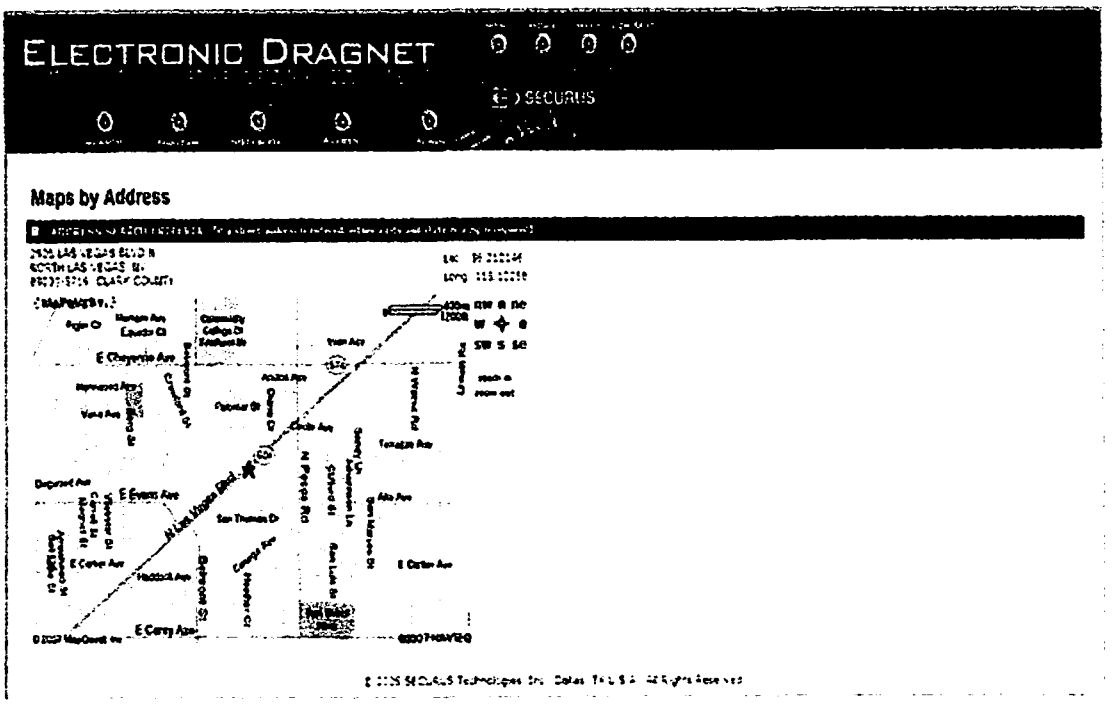
Reverse Number Lookup

An investigator can select and lookup the owner and address of a called phone number, either by entering it directly into the application or by "selecting" (i.e. clicking on) the reverse number lookup icon next to a displayed phone number. This feature searches a wide variety of published phone number lists in order to return the most relevant owner and address information possible.



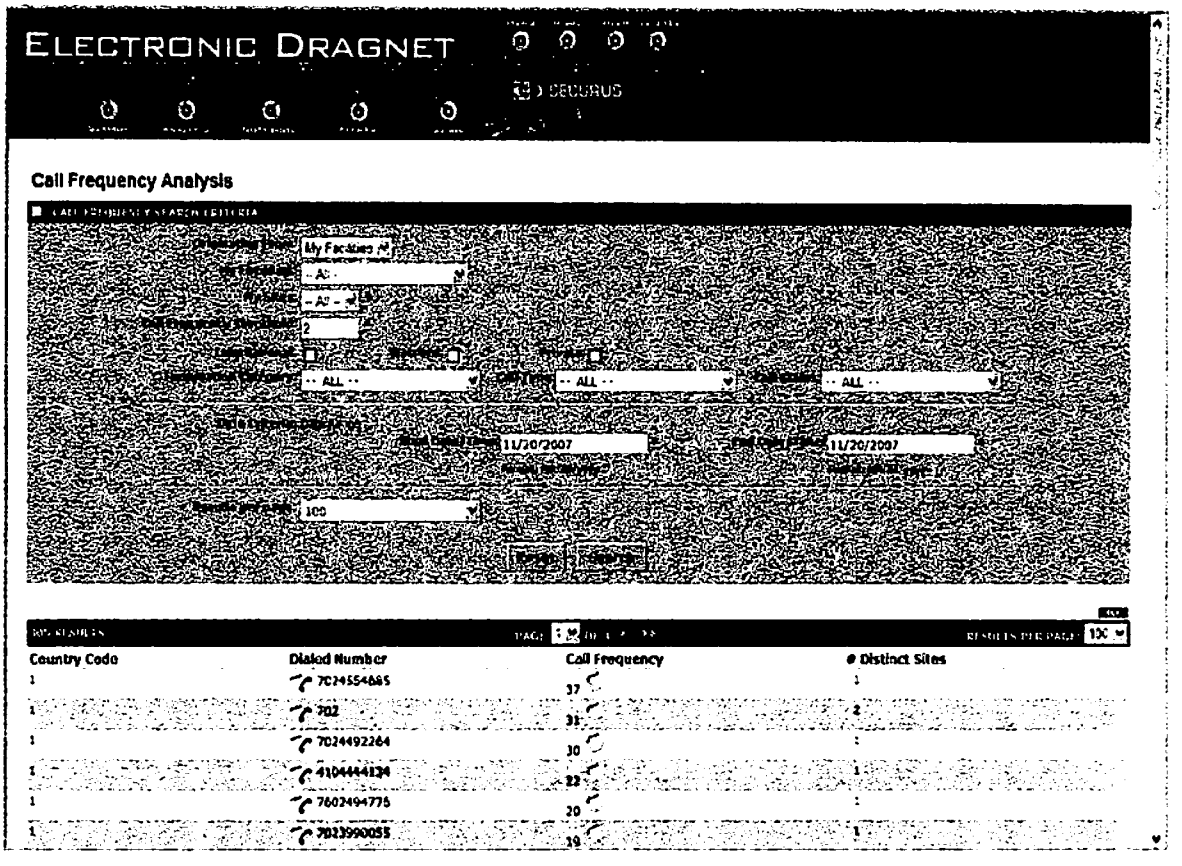
Simply selecting the icon next to the phone number provides the investigator the phone number owner name and address.

Searches
Electronic Dragnet Basic also produces on-the-fly maps; providing visual address information, including latitude and longitude coordinates complete with driving directions.



At any time, an investigator can display a history of their recent searches and associated results.

Analysis
The investigator also has the ability to initiate a query that immediately displays a list of frequently called numbers, by date and time, from their facility.



The call frequency report displays the number called, call frequency and number of sites where that number has been dialed from. This report can also be printed as a PDF for easy printing.

Platform for the future
SECURUS' centralized hosted application platform provides Electronic Dragnet a platform to host a continually evolving suite of new data sources and intelligence tools ensuring that investigators have access to the best available resources in order to prevent and solve crime.

Electronic Dragnet is SECURUS' Investigate Portal for the future. In the first quarter of '08 we will be implementing functionality that includes:

- **CDR Search - National Number Search**
- **Covert Alert**
- **Live Monitor**

- **Record to CD**
- **Scan Patrol**

Currently SECURUS is actively pursing many biometric and analytic tools. Our development plans include the possibility of many exciting "Advanced"[1] options for Electronic Dragnet users including:

- **Notebook Advanced**
  - **Case Information Sharing**
  - **Add notes to individual calls**
    - **Call Summaries**
    - **Investigative Notes**
- **Information Sharing Capabilities**
- **Word Spotting**
- **Person Search for public record information**

5.20
Inmate Account Information

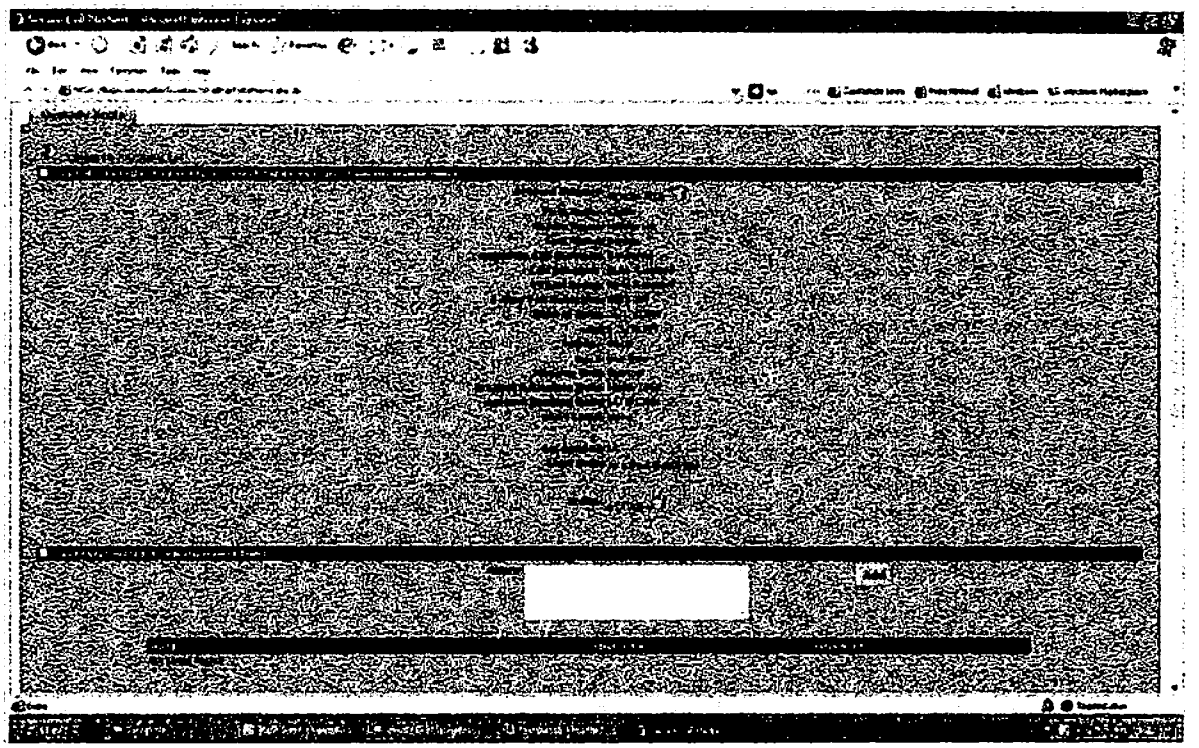
5.20.1 The Proposal shall describe the options for DOC concerning inmate account information. This description shall include, but not be limited to, such items as PIN, length of inmate name fields (first, middle, last), identifier of DOC facility, comments field, language preference field, account activation date, date of arrival, and current status.

☑ **SECURUS has read and will comply.**

Secure Call Platform optional fields concerning inmate account information are: Account Number/PIN Number, First Name, Middle Name, Last Name, Maximum Call Duration, Call Schedule, Virtual Group, 3-Way Call Detection, Date of Birth, Social Security Number, Gender, Race, Housing Unit, Account Activation Date, Account Booking Date, Alert Level, Suspension Status, Start Date of Suspension and End Date of Suspension.

Additionally, a comment field is available to add specific information pertaining to an account/PIN. Language preference/options are provided through the platform during the process of the call.

[1] Advanced options will be available to all Electronic Dragnet Basic users for an additional fee.



5.20.2 The proposed ITS shall provide alert levels to be placed on an inmate's account information. Such alert levels shall be viewable in real time mode by the system administration terminal or by printed report.

☑ **SECURUS has read and will comply.**

Through Secure Call Platform's user interface authorized Alaska DOC personnel are able to configure and set real-time watched number alerts for numbers under surveillance, or for numbers tied to illegal activities, and covert alerts for remote monitoring of live calls in progress. Alert information is also viewable on printed call detail reports.

5.20.3 The proposed ITS shall allow DOC to restrict an inmate under disciplinary action from placing all calls assigned to his particular PIN with the exception of privileged numbers.

☑ **SECURUS has read and will comply.**

5.20.4 The Proposal shall state the maximum number of telephone numbers assignable to an inmate's account.

☑ **SECURUS has read and will comply.**

SECURUS currently has clients who use up to 30 telephone numbers per inmate, but this number is customizable for each client and could be higher if necessary.

5.20.5 The proposed ITS shall provide the preference of English or other language voice messages or prompts depending on an inmate's account information. The default setting for each inmate shall be English until flagged by DOC personnel to another language.

☑ **SECURUS has read and will comply.**

5.20.6 The proposed ITS shall provide standard language prompts other than English. Any language provided shall be controlled by the inmate's account information. The Proposal shall provide a list of languages available with the proposed ITS.

☑ **SECURUS has read and will comply.**

The Secure Call Platform is capable of providing message prompts in English and Spanish. An inmate may select a specific language at the beginning of the call process by dialing a single digit. This will initiate the selected language prompts to the inmate. If desired, the language selection for the called party may be preset in the system database. If additional languages are required, they may be developed for specific customer needs at no cost.

5.20.7 The proposed ITS shall be capable of assigning an inmate's account to an individual telephone or group of telephones so that the inmate's account may only place calls from those designated telephones. These telephones shall still be capable of being used by inmate accounts not specifically assigned to them.

☑ **SECURUS has read and will comply.**

5.21
Additional Operational Requirements

The proposed ITS shall be capable of being configured to control the amount of time between inmate-completed calls. The proposed ITS shall be capable of placing time limits on calls. DOC shall be capable of enabling and disabling this feature. This time interval shall be configurable by minute increments.

☑ **SECURUS has read and will comply.**

With SECURUS' calling platform, inmate call duration per call is programmable by inmate but not the time between calls. A default time limit is provided for the entire system and individual groups can be added for specific telephones as well as inmates within a group. The time limit may be changed for each active phone, individual inmates, and/or the entire system. Additionally, the Alaska DOC can choose to limit the number of calls per day or week, hours during which calls can be made, and the type of calls that can be made during each time period. However limiting time between calls is not available at this time. SECURUS is currently developing this feature to be provided in the Secure Call Platform and expects general availability by the third quarter of this year.

5.22
Transition And Implementation Requirements

DOC presently has an ITS system. The Proposal shall address the transition from the existing ITS to the new ITS at all DOC institutions listed in Table One of this RFP. DOC realizes that some "down time" will occur during this transition but the Offeror shall propose an implementation plan that reduces this "down time" and allows for a smooth progression to the new ITS.

☑ **SECURUS has read and will comply.**

5.22.1 The Offeror shall furnish or cause to be furnished, all labor, supervision, equipment, materials, and supplies necessary to install the proposed ITS systems.

☑ **SECURUS has read and will comply.**

5.22.2 The Proposal shall provide a transition and implementation plan which shall include, but not be limited to, the following components:

A. A time line for all facilities;

B. Transition procedures from the existing ITS system to the new ITS System;

C. Staffing requirements of DOC for each facility;

D. Responsibility of DOC staff at each facility; and

E. Make-up of the Offeror's implementation team.

☑ **SECURUS has read and will comply.**

SECURUS has the distinct advantage as being the manufacturer of the current platform installed throughout the Alaska DOC as well as the manufacturer of the Secure Call Platform (SCP) proposed in our offer. As the manufacturer of both platforms, SECURUS can insure a smooth transition in maintaining and importing existing critical data from the current CAM platform into the new SCP with little to no impact in inmate telephone calling privileges.

SECURUS has a significant amount of experience spanning two decades of installing inmate telephone systems in a Department of Corrections environment. During the installation of each institution, SECURUS will work closely with the Alaska DOC to convert all telephones to the new services in a secure and timely manor. It is our intent to install new telephone equipment, provision and test SCP voice services at each institution, import all inmate profile information and then move cable connections from old to new services. Once all services at an Institution are cutover to SCP, a technician will be required to enter each location in which an inmate telephone is installed to conduct a final test as well as re-affirm location of the station set.

A preliminary project plan for the inmate phone implementation is included in *Attachment H – SECURUS Preliminary Project Plan.*

Project Controls and Quality Checks
Timely execution and completion will be monitored by using scheduled completion dates in correcting implementation or operational problems, as well as problems reported through SECURUS trouble reporting system. Summary reporting, trend analysis, and schedule monitoring will facilitate tracking problem correction.

Other less formal reviews of installation status are held throughout the installation. Operations staff meetings provide the Implementation Manager. Installation Manager and Project Manager with periodic status, and allow coordination and dissemination of the information to SECURUS Installation field technicians.

Transition Period with Minimum Service Disruptions
Because SECURUS is the current provider, transition downtime will be minimal, if any. By installing all SECURUS ITS equipment and circuits prior to the cutover date, usually one to two weeks in advance of the cutover date, this allows for all systems, circuits, etc., to be fully tested. By fully testing prior to cutover, there will be no risk of service interruptions due to the changeover to the new SECURUS ITS system. The SECURUS team has used this process with much success throughout their many multiple site accounts in the US & Canada.

SECURUS will have installed and tested all necessary equipment and circuits prior to the actual cutover date. There will not be any interruption of service. The cutover may be conducted during the time the facility has all phones off, i.e., a count time, prior to the phones coming on at the beginning of the day or after the phones go off for the day. This will minimize any downtime for the facility.

Software Programming and Preparation
After meeting with personnel from the Alaska DOC, internal meetings will be held between Project Management and Install Team to review the validation process that will be used to ensure that the system conforms to the functional facility requirements.

Prior to shipment systems are fully tested and that the ITS system can be successfully implemented at the Alaska DOC sites. Hardware design will be performed for each site to be installed. After the site surveys are confirmed all site requirements will be identified and a Bill of Lading (BOL) will be prepared. The BOL will be provided to the Alaska DOC to ensure all parties agree to the items and their quantities. The system equipment is assembled, and forwarded to a staging and testing area prior to shipment. The system is typically shipped two weeks prior to cutover.

Testing

SECURUS will perform comprehensive testing to be sure all features and functions are working properly before cutting the system. A second round of testing will be conducted as soon as the system is cut, if the system is accurately processing calls with all required security a 24 hour burn in period will begin.

Test calls are placed from each station port to each trunk. The network integration is validated through a battery of tests that include frame testing and file transmission.

Individual component tests will be completed by the project manager and field technicians prior to beginning the 30-day operation period, including:

- **Place local Calls and listen to voice prompts**
- **Select Spanish prompts**
- **Place intraLATA, and interLATA calls**
- **Attempt to call blocked numbers**
- **Print sample call detail reports at the workstation**
- **Verify that site received user manuals**
- **Confirm and Test Prepaid calling**
- **Attempt a 3-Way call**
- **Listen/monitor and active call**
- **Query Recorded Call information**
- **Place a call to a privileged number**
- **All recording and monitoring functions**
- **Assign and test PIN accounts. Complete Test calls for PINs.**

The major tasks involved in a standard ITS installation are detailed below.

Task Name
Contract Signed
Implementation Meeting Held with designated Alaska DOC personnel and SECURUS Project Team Personnel • **Establish site contact personnel from the Department** • Establish ITS rollout schedule and approval by Alaska DOC • Finalize feature set selection • Verify Findings from Site Surveys of All Locations • Identify special need phones, i.e. TTY/TDD, portable/moveable phones • Review Alaska DOC policy and procedures/DOC, security clearances for SECURUS installation teams
SECURUS Project Team Meetings

Task Name
Conversion Plan Evaluated & Adjusted as Necessary During Weekly Internal Conference Calls Through-out Project Duration • Confirm install dates with Master Scheduler • Review Final Plan with Installation Teams • Confirm Install Support • Confirm Shipping • Confirm Training
Order/Install Lines for all locations • T1's/Analog Lines/Frames
Feature Selection Confirmed
Obtain Line Numbers and Confirm Orders and Due Dates with Local Exchange Company
Branding Messages Developed
Configure ITS
Quality Control ITS test • Feature testing • System testing • Load testing * All quality control is conducted in +Dallas prior to ship.
Package & Ship Equipment to Delivery Location
Installation of ITS • Receive and inventory equipment • Build equipment • Prepare to cut ITS – Power-up ITS – Install workstations – Conduct install test – Coordination with Install Support – Install blocked number table, free numbers, and inmate PINs/PANs • Replace inmate telephone sets
Cutover of ITS • Notify facility that cutover will occur and gain Site/Central office approval to proceed • Cutover system at agreed upon time to minimize disruption • Notify facility of cut
Quality Assurance of ITS and Acceptance Testing Complete
Training of Facility Personnel

5.22.3 The Proposal shall provide an implementation plan that shall include a detailed explanation of the following items:

A. Pre-installation procedures for each DOC facility;

B. Pre-installation procedures for the complete ITS system;

C. Network service coordination requirements;

D. Software programming;

E. Equipment delivery schedules;

F. Equipment security procedures;

G. Equipment/system installation procedures;

H. Station Equipment installation procedures;

I. ITS system testing;

J. Offeror central site planning and implementation; and

K. Actual ITS system cutover to service.

☑ **SECURUS has read and will comply.**

A preliminary project plan for the inmate phone implementation is included in *Attachment H – SECURUS Preliminary Project Plan.*

5.22.4 The Offeror shall remove the existing Inmate Station Equipment (Telephones) in all DOC facilities listed in Table One of this RFP and replace them with new telephones at no cost to DOC. Existing equipment is the property of the current contractor, Evercom Systems, and must be returned to them at Evercom expense.

☑ **SECURUS has read and will comply.**

5.22.5 In the event of a problem or question of continuity arising during installation of the proposed ITS system, the Offeror shall make provisions for joint testing of the ITS system by the Offeror and DOC at no additional cost to DOC.

☑ **SECURUS has read and will comply.**

5.22.5 The Offeror shall be responsible for the generation and creation of the system database(s) required to provide a fully operational ITS. As requested, the DOC shall provide the Offeror with appropriate information.

☑ **SECURUS has read and will comply.**

5.22.7 The Proposal shall describe how the current system database information, including inmate profile and call records, will be retained during conversion to the new ITS system.

☑ **SECURUS has read and will comply.**

One of the main advantages with selecting SECURUS is ease of replicating all historical inmate profile information that resides in the current CAM system into the newly offered Secure Call Platform. The CAM data structure is completely compatible with Secure Call Platform without the need to convert the data from one proprietary format to another.

5.23
Implementation Team

5.23.1 The Proposal shall specify the members of the team and their responsibilities for installing the proposed ITS at each DOC facility.

☑ **SECURUS has read and will comply.**

Position	Name	Responsibilities	Qualifications
Installation Technician	Aaron Bacher (Install Manager)	Installing and testing the system and network.	Telephony (DS3, DS0, T1 64K, 56K, AMI, and B8ZS), Telephony troubleshooting. BICSI cable requirements and load limit (loop) standards, Adtran 550/624 programming and product limitations. IP configuration @ Gateway and Subnet level on Cisco products. Functional Knowledge of; Sybase / SQL, Windows Networking knowledge of NT, 2000, XP. Troubleshooting skills of common Networks Class A and B. Knowledge of IIS web servers, Apache, Unix and Betrieve, CompTIA A+, T1/56K/Pots circuit testing, Cable management and LAN/WAN testing.
Project Manager	Paula Parsons	* Manage the extraction and conversion of existing client data. * Manage software installations and applications. * Manage installation process of phone, computer, etc systems for our clients from beginning to end. * Manage Project scope and conformance with System Quality Control, Statement of Work, Documentation, Implementation and Customer interfacing. * Work with management and technicians to set project objectives, priorities and deliverables. * Identify project road blocks and work with management and team members to resolve them. * Perform budgeting (cost/quality control) and scheduling processes to ensure customer satisfaction. * Ensure successful execution of installation programs. * Manage the customer delivery and follow correct policies and procedures in the building of our equipment – management of all outsourcing activities. * Ensure all clients programming, connectivity and configurations meet company standards. * Manage the project internally and schedule resources for timely project	* 5+ years of Project Management experience in the successful management of software conversions. * 5+ Years within the Telecommunications industry. * Broad understanding of enterprise IT installations and their requirements. * Strong knowledge of Project Management principles, practices, techniques and tools. * Strong Customer Service Skills and the ability to interface with customers. * Outstanding documentations skills, analytical skills, organizational skills and be detail oriented. * Working in a fast paced environment meeting and exceeding the needs of our customers.

Position	Name	Responsibilities	Qualifications
		deadlines.	
Installation Support	TBD Based on Availability	Monitor the system and network to detect any problems and remotely correct and identify problems without the need for dispatching a field/repair technician to the DOC's facility. If the Installation Support Specialist cannot remotely correct or repair the system problem, they will be responsible for dispatching the appropriate field repair/site technician to the facility to make the repairs as necessary and track the issue through to completion, offering assistance as necessary. Provide detailed troubleshooting/ problem resolution as well as root cause analysis for all service issues. Handle inbound call traffic to resolve customer problems. Monitor all aspects of Network, Systems, facility infrastructure and provide outbound communications. Effectively communicate status to customers and internal staff on open issues or questions. Provide all levels of support to resolve complex, technical customer problems. Network circuit repair on Cisco/Adtran/Juniper platforms. A key responsibility is the documentation of trouble resolution through the use of the HEAT trouble tracking and ticketing system. Ensure issue resolution is verified and meets with the customer's satisfaction for all tickets before closure. Work with Field Technicians to fully resolve any and all problems.	This position will have expert knowledge of media types from ADSL through OC-12. UNIX/NT/Windows administration of production servers includes installations, maintenance of OS, etc.
Field Service Technician	Jasen Kitner	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. A FST is dispatched from location to location or serves as the On-Site FST for a particular customer campus. Installs, maintains, programs and repairs telecommunications hardware, associated LAN/WAN/Networking hardware/software, various electronic equipment and wiring per specifications and operational procedures. Works on a one-on-one basis with sworn facility staff, civilian facility staff, the inmate population and the family members of inmates to resolve questions and	The Field Services/Site Technician will CompTIA A+ Certification, as well as, a minimum of 2 years experience working with Cisco based routers, switches and PIX firewalls.

Position	Name	Responsibilities	Qualifications
		concerns regarding billing, training, technical support and operational issues. Monitors and tests equipment according to published equipment standards. Gather, update, record and maintain related data and/or statistics. Interface with all internal SECURUS organizations, various vendors and contractors for problem solutions. Assess and respond to situations where standard procedures have failed in isolating or resolving problems.	
Customer Service Representatives	Varies	Assist customers via telephone on both inbound and outbound calls using a professional approach, including appropriate grammar and language skills. Facilitate the establishment of new accounts by obtaining and documenting the required information for customers to open a new account.	Each Call Center Representative is specifically trained to handle the unique issues surrounding inmate calling and is supported by a full-featured customer account management and billing system on which each Call Center Representative is thoroughly trained. Using the specialized skills obtained through Correctional Billing Services' training programs that focus on the needs and issues of friends and families of inmates, the Call Center Representatives are fully equipped to professionally handle all matters relating to services offered by SECURUS.

5.23.2 The Proposal shall state the requirements and responsibilities of DOC's implementation team.

☑ **SECURUS has read and will comply.**

At the initial meeting, SECURUS and the Alaska DOC will develop and finalize the ITS implementation schedule.

Weekly meetings with the Alaska DOC and updates to Project Management Plan will follow. To allow timely system installation and implementation, Alaska DOC staff at each facility will be made aware of the installation schedule to grant the SECURUS implementation team access to specific facility areas.

At the end of each installation, the Project Manager, Installation and Operations Manager will compare actions, efforts and time expended to that point. If there are significant variations from the plan a risk will be identified and tracked. The plan will be evaluated and updated based on performance. The measure provides an accurate measure of whether actions are being worked or not.

Items that are late will be investigated and brought to closure as soon as possible.

The Alaska DOC Central Office and/or the Alaska DOC facility responsibilities will include:

- **Presence at implementation meetings**
- **Perform security clearances on SECURUS personnel**
- **Establish contact personnel and Alaska DOC policies & procedures**
- **Confirm installation to proceed**
- **Warden approval to proceed to cutover and agree on off hours to complete to minimize service disruption**
- **Business hour access to SECURUS implementation team**
- **Accept Delivery of needed installation equipment upon scheduled arrival**
- **Participate in scheduling of Training classes to the Alaska DOC staff**
- **Acceptance phase This measure will report on the number of action items, which are 1 to 30 days late**
- **Allow access to facilities for location clean-up**

The SECURUS Account team will be available to meet monthly with the Alaska DOC staff for the purpose of presenting ITS prior month's maintenance reports mentioned in the previous section and to discuss resolutions to issues and concerns. These meetings will be scheduled at the discretion of the Alaska DOC.

5.23.3 The Offeror shall assign one project manager to oversee the ITS. This project manager shall act as a single point-of-contact for DOC during the life of this ITS system implementation.

☑ **SECURUS has read and will comply.**

The Project Manager will be Helen McCoy.

5.23.4 The Offeror shall warrant that each member of the implementation team who will service the proposed ITS system has been fully trained and certified by the manufacturer as qualified to service the proposed ITS.

☑ **SECURUS has read and will comply.**

All field technical personnel are factory trained on our internally designed and developed ITS system. In addition to the factory training, 33 of our field technicians are A+certified. After the completion of a course provided by CBT Direct, the technicians are then certified by Thomson Prometric. A+ certification validates that a technician processes the latest skills needed by today's

computer support professionals. It is an international, vendor-neutral certification recognized by major hardware and software vendors, distributors and resellers. A+ certification confirms a technician's ability to perform tasks such as installation, configuration, diagnosis, preventive maintenance and basic networking. The exam also covers domains such as security, safety and environmental issues and communication and professionalism. A+ certification ensures the right people have the right skills.

The following table list of the specific certifications and professional affiliations held by the base of our employees:

Microsoft - Certified Office Specialist
Microsoft - Certified MCT
Microsoft – MCSD
Microsoft – MCDBA
Microsoft - Certified MCSE
Microsoft – Certified MCP
Microsoft – Certified MCAD
Adobe - Certified Professional
Adobe – Adobe Certified Expert in Photoshop
Adtran Certified Solution Expert
Certified Internet Webmaster
Certified CNE
Certified PMP
Certified CNI
Certified ECNE
Certified Master CNE
Certified CCSI
Certified CCNA
Certified CCNP
Certified CISSP
Certified Clear Case: UNIX Windows
Certified Java Programmer
Certified Web Component Developer for J2EE
Certified Passport Switch 6000/7000
Certified Passport Switch 1000/8000
Technical Writing Certification
Training and Development Certification
A+
N+
OCP – Oracle Certified Professional
OCA – Oracle Certified Associate

Professional Associations:

Society of Technical Communications
Usability Professionals
Microsoft Certified Trainer Advisory Council
CNE Professional Association
E-Learning Guild
American Society for Training and Development
APICS Association for Operations Management
ISM – Institute for Supply Management

5.24
ITS System Testing

The Proposal shall provide a comprehensive functional test plan to assure DOC of the ITS system's readiness to accept inmate call out traffic. This test plan shall include a checklist of items to be performed by the Offeror's implementation team and verified by the DOC staff.

☑ **SECURUS has read and will comply.**

The SECURUS Acceptance and Test Plan provides a complete and comprehensive acceptance plan for the proposed system. This may be used in every installation for the Alaska DOC. The acceptance plan is the standard against which acceptance is typically measured. SECURUS looks forward to working with the Alaska DOC in developing a specific plan that meets all of the mutually agreed upon criteria.

Testing
Each system is placed under 'stress-testing' before it leaves the production facility. This testing procedure simulates that all ports on the system are in constant use 24 hours straight, for 7 days. The system is again tested onsite to insure total functionality. Test calls are placed from each station port to each trunk. The network integration is validated through a battery of tests that include frame testing and file transmission.

Individual component tests will be completed by the project manager and field technicians prior to beginning the 30-day operation period, including:

- **Place local Calls and listen to voice prompts**
- **Select Spanish prompts**
- **Place intraLATA, and interLATA calls**
- **Attempt to call blocked numbers**
- **Print sample call detail reports at the workstation**
- **Verify that site received user manuals**
- **Confirm and Test Prepaid calling**
- **Attempt a 3-Way call**

- **Listen/monitor and active call**
- **Query Recorded Call information**
- **Place a call to a privileged number**
- **All recording and monitoring functions**
- **Assign and test PIN accounts. Complete Test calls for PINs**

A standard checklist is included in *Attachment I – SECURUS Test/Acceptance Plan.*

5.25
ITS System Acceptance

The Proposal shall provide a comprehensive acceptance plan for the ITS at each DOC facility. ITS system acceptance shall be determined by a consecutive 30-day period during which the system shall function "error free." The Offeror shall work with DOC to determine the actual definition of "error free" operation. Failure of the system to meet mutually agreed upon acceptance criteria for more than 30 days may result in DOC requesting replacement of that particular system. Additional acceptance requirements are stated in Section 3.5.1 of this RFP. Where a conflict exists, the more stringent requirement as determined by the DOC shall apply.

☑ **SECURUS has read and will comply.**

A standard checklist is included in *Attachment I – SECURUS Test/Acceptance Plan.*

5.26
ITS System Documentation

5.26.1 At the completion of the ITS system installation and implementation, the Offeror shall provide a complete set of ITS system reference manuals that must include information specific to the installation at each DOC facility.

☑ **SECURUS has read and will comply.**

5.26.2 The Offeror shall supply trouble logs for all problems reported on the ITS system on an as needed basis.

☑ **SECURUS has read and will comply.**

5.26.3 The Offeror shall supply all necessary documentation to the DOC site administrator relating to maintenance contact numbers, maintenance reporting procedures, and maintenance escalation procedures, etc.

☑ **SECURUS has read and will comply.**

5.27
Training Requirements

It is critical to the success of the installation of the ITS that DOC personnel be thoroughly trained in various aspects of the system operation. Therefore, the Offeror shall provide a complete training schedule based on the following requirements.

☑ **SECURUS has read and will comply.**

SECURUS will provide system training, including documentation, covering the Secure Call Platform. All training is provided by experienced employees of SECURUS. At the end of the training module, including the completion of extensive hands on practice with the Windows-based user interface, participants will be able to perform the functions necessary to the basic operation of the Secure Call Platform. Training on the SECURUS Secure Call Platform, including supplemental and refresher training, is provided at no cost to the Alaska DOC.

SECURUS offers an extensive training program, along with detailed documentation and automated voice instructions, in order to prepare the facility personnel and the inmate population for the use of the inmate telephone system. SECURUS' training program enables facility personnel to take advantage of the system's features beginning from the day of installation.

SECURUS will provide at least two days of on-site, classroom style training for various levels of facility staff. The training emphasizes hands on demonstrations to familiarize participants with the SECURUS Secure Call Platform. The courses are designed to encourage participants to practice the skills necessary to perform their daily functions on the SECURUS Secure Call Platform. As the system is a Windows based program, most participants find it easy to maneuver through the programs almost immediately.

Additionally, SECURUS will work with you to tailor our efforts to meet your training needs. We can also do separate classes for different groups of individuals to ensure that we are matching our training to each groups requirements and focus on their individual needs.

Training Course Elements
SECURUS is committed to ensuring that the users of the system are provided with ongoing training that will help them maximize the investigative and administrative potential of the system. The following table details the standard system training course elements that SECURUS will provide at no charge. In addition, our customers are provided with detailed system manuals and learning tools that will further complement their system administration capabilities.

Course Element	Description
System Components: Purpose and Operation	Participants learn what a wide area network (WAN) and a local area network (LAN) are, and how they relate to the components of the system. All components of the system will be discussed, as well as the centrally located system server and backup system(s).
Secure Access: Multilevel Password Security Features, Functionality and Operation	Participants will be instructed on how to set up and assign different or specific access levels to authorized individuals. Participants will also learn how to modify initial access levels and or input additional levels based on facility clearance objectives and designated entry to each application. The facility administrator has the ability to determine system accessibility by assigning passwords and security levels to authorized personnel. Multi-Level access applies to each application of the system with three primary levels – Low, Medium and High. Participants will be trained in the manner for which appropriate application levels are applied.
System Live: 1. Call Monitoring and Disabling 2. 'Live' Call Activation 3. Remote Access 4. Disabling 5. Investigative Tool	LIVE: Visual and Audio call monitoring will be described with specific instructions on how to activate the primary functions of this application. Specific features of the 'Live' monitoring screen will be discussed in detail to include: • column headings • manipulation of the information order • 'hot' keys for disabling/enabling ports • multiple party monitoring REMOTE: The monitoring application tools will be discussed to include on-site 'Live' monitoring and the remote access capabilities specific to performing tasks related to the 'Live' call retrieval and forwarding functions. DISABLING: Authorized personnel will also be trained in the area of phone control for the purpose of disabling individual or multiple ports when immediate action is required. INVESTIGATIVE: The potential to deter and control crime within the facility and outside the facility through the use of call monitoring will be discussed. Actual customer experiences will be shared with the participants.

Profiler:
PIN & PAN Setup/Maintenance.
Prisoner Identification #s
Call Restrictions/Privileges Personal Allowed # Lists
Global Assignment
	Participants will learn how to:
	• Establish an inmate PIN record with specific number assignments, time restrictions and audit trail of calls
	• Define a Personal Allowed Number list with specific number restrictions and called party association
	• Assign Private Number Status for attorney/client privilege (disables recording and monitoring capabilities)
	• Assign 'Watched' Number Status
	  • Remote and on-site alerting capabilities
	• Apply Call Restrictions per PIN
	  • Time of day restrictions
	  • Call limitations based on daily, weekly and monthly
	  • Special calling privileges
	• Access record for editing and modifications

Course Element	Description
	• Global number assignment
Watched Number Alert: Audible watched number alert	Selected participants will be instructed on how to designate specific numbers as 'watched' through the 'Watch Alert' feature of the Number Restrict Editor application.
Covert Alert: Remote Live Monitoring of Calls	Participants will be instructed on how to set up and establish remote call forwarding and monitoring for those numbers that are under surveillance. Participants will learn how to enter new numbers and the destination number to which the call will be forwarded once in progress. Additionally, participants will also learn how to display the active/inactive list of those numbers assigned a 'watch' status.
Call Playback Function: Recorded Playback Copy Function Restore Function	PLAYBACK: The participant will be taught how to selectively retrieve and listen to a pre-recorded conversation that is resident on the hard drive, backed-up to AIT device or other archival device. COPY: Participants will be instructed in how to copy a pre-recorded conversation to a CDR device that offers enhanced portability and a valuable tool for building a library of evidence. RESTORE: Instruction will be provided on the restorative capabilities of the system relative to the tape backup function.
Recorder Application: Hard-Drive Capacity Back-up Function Labeling Function	HARD-DRIVE: The participant will be versed in the storage capacity of the hard-drive with specific instruction on the importance of maintaining a tape drive back-up. BACK-UP: Instruction specific to the back-up process and storage life of the calls. LABELING: Participants will be instructed in the proper labeling of storage devices for the purpose of recall and playback of audio calls.
Three Way Call Detection: Methodology Options Available On-Site Controls	METHODOLOGY: Participants will be instructed in the methodology employed to reduce the incidence of 3-Way calls. OPTIONS: Instruction will be provided on the options (tag line messaging, call termination, etc.) available for handling potential 3-Way calls. CONTROLS: Participants will learn how to adjust the sensitivity settings to reduce the incidence of flagging calls that are not 3-Way attempts.
Restrict Number Editor: Search Parameters New Number Assignment Editing/Delete Restrictions Restrictions & Assignments Validation Codes	SEARCH: Instruction will be provided on the restriction feature, which allows authorized personnel to search, retrieve, review and edit number restrictions. The use of this feature as a tool to officers and investigative personnel will be described in detail. NEW: Instruction will be given on how to add a new number and apply restrictions to it such as 'Watched', 'Free', 'Call. Block' and 'Private'. Use of the description field for comments or reasons for the restriction will also be discussed. EDIT: Participants will also be instructed on how to identify, edit and delete a telephone number and/or restrictions that has been previously entered in the system. RESTRICTIONS: Participants will review each of the number restrictions and assignments available through this

Course Element	Description
	application to include call blocks, harass and PERMAblock function, free, private and watched status, and the wildcard feature. VALIDATION: Review the validation process. The associated codes and status of the number will be included.
Investigative Reports: Tracking/analyzing inmate call patterns Report Types Parameter Fields Selective Grouping Global Restrictions	REPORTS: Participants will review each of the 15 standard reports with discussion on the capability for generating user specific reports. PARAMETERS: The participant will be versed in the parameter fields relative to each report and how to generate a report with user defined information and report content. The participant will be informed of the investigative values of the report application. The parameter fields include information relative to each telephone, location, destination number, date, PIN, call duration, call type, frequency of calls, etc. SELECTIVE: Participants will receive instruction on how to perform group or individual call searches from a single application. GLOBAL: Participants will also learn about the value added function of the global administrator for number restrictions.
Call Tracker: Case notes with embedded conversations Investigative Tool Case Management	Participants will be instructed in how to establish an investigative log of calls with specific tracking identifiers. The instruction will also include the ability to search, edit and expand existing record logs and the value it offers the investigative unit for case management.
Transporter: 'True Portability with embedded call detail	Authorized personnel will be instructed in the methods to copy one or multiple calls to a CD that can be played on any PC without system software. Participants will also be taught how to create a CD for use on any audio stereo device (e.g., 'Boom Box' or car stereo system).
Optional Calling Methods: Debit Based Platform Prepaid Card CBS Account Prepayment	In addition to collect calling, additional calling options are available through the system. Participants will be provided with an overview of each option and the value it offers. DEBIT: The system offers a fully integrated debit based calling platform that offers additional tracking controls of the inmates calling activities. PREPAID: Cards can be purchased and then resold through the commissary to allow inmates to prepay for calls placed to friends and family. CBS: Family and friends have an option to prepay their phone charges through our dedicated customer care center.

5.27.1 **The Offeror shall provide training to DOC at no cost.**

☑ **SECURUS has read and will comply.**

5.27.2 The Offeror shall provide end-user training on site at the various DOC facilities.

☑ **SECURUS has read and will comply.**

5.27.3 The Offeror shall provide on-site training for various levels of DOC staff including part- time and full-time system administrators, special investigators, and data entry specialists.

☑ **SECURUS has read and will comply.**

5.27.4 The Offeror shall provide training for all assigned ITS system users on the following matters:

A. How to create, delete and modify inmate records;

B. How to generate appropriate system reports;

C. How to maintain alert levels and respond accordingly when these levels are exceeded;

D. How to change inmate restriction levels;

E. How to initiate system restrictions including the shutting down of individual inmate telephones, groups of inmate telephones or the entire facilities systems; and

F. How to use any filters to further refine searches for reports.

☑ **SECURUS has read and will comply.**

5.27.5 The Offeror shall provide training on all components of the ITS.

☑ **SECURUS has read and will comply.**

5.27.6 The Offeror shall provide full training on the provided recording equipment including the live monitoring of inmate calls, playback of archived calls and the transfer of calls to other media for playback at off-site locations.

☑ **SECURUS has read and will comply.**

5.27.7 The Offeror shall provide refresher ITS system training for existing DOC personnel when required by DOC and at no cost to DOC.

☑ **SECURUS has read and will comply.**

5.27.8 The Offeror shall provide additional training for new DOC personnel when required by DOC and at no cost to DOC.

☑ **SECURUS has read and will comply.**

5.27.9 The Proposal shall describe any advanced ITS system training that may be available to DOC personnel whether provided on-site at an DOC facility or off-site at the Offeror's training facilities.

☑ **SECURUS has read and will comply.**

5.27.10 The Proposal shall include the name and the title of the person who will have the overall responsibility for training.

☑ **SECURUS has read and will comply.**

Karen Svensson, Technical Education Process Manager, will have overall responsibility for training.

5.27.11 Written material utilized in the training program shall become the property of DOC upon completion of the training sessions.

☑ **SECURUS has read and will comply.**

5.27.12 The proposed ITS shall provide for on-line help for ITS operation, administration, reporting and management functions.

☑ **SECURUS has read and will comply.**

5.28
Post Installation and Expansion Requirements

5.28.1 DOC may require the addition of equipment at its facilities after the original installation of the proposed ITS. The Offeror shall install additional equipment within 30 days of notification from DOC authorized personnel. This equipment and installation shall be at no cost to DOC.

☑ **SECURUS has read and will comply.**

5.28.2 The Offeror shall be responsible for making all ITS system modifications necessary to allow inmates to place calls as industry dialing requirements change, at no additional cost to the DOC.

☑ **SECURUS has read and will comply.**

5.28.3 The Offeror shall be responsible for complying with and updating the ITS system for any regulatory changes and requirements during the Contract term, at no additional cost to DOC. These regulatory changes and requirements include federal, state, county and municipal modifications.

☑ **SECURUS has read and will comply.**

5.28.4 All call processing and call rating information shall be kept current by the Offeror to ensure the ability to place calls. This information includes, but is not limited to, local exchanges, area codes, vertical and horizontal coordinates, and any other information necessary to accurately process and rate calls. The Offeror shall provide DOC with rating information for all cases when requested by DOC.

☑ **SECURUS has read and will comply.**

5.28.5 DOC reserves the right to renegotiate the Contract in the event that, (A) calling rates become noncompetitive and/or (B)advances in technology, equipment and/or software are such that retaining existing equipment and/or software would not be in DOC's best interest. (C) if the number or minutes of calls increase substantially due to unforeseen circumstances.

☑ **SECURUS has read and will comply.**

5.29
Prepaid Calling Requirements

5.29.1 The proposed ITS must provide for inmate use through prepaid calling in addition to collect call mode. The Offeror shall develop a prepaid calling plan that shall allow for the establishment of a new prepaid account with the Contractor to be funded by a person(s) on the inmate's calling list who is duly approved by the DOC to receive calls from an inmate, as a voluntary alternative calling and payment procedure to the standard collect call procedure. Those accounts shall be established without an account set-up fee. This pre-paid program will not require staff time, maintenance, or cost from the DOC. The Offeror shall be responsible for providing staffing and any other resources necessary to implement a prepaid calling plan. The rates for consumer charges under the prepaid calling plan are set forth in Sections 5.28.8, 5.28.9, and 5.28.11. The commission owed to the DOC under the pre-paid calling plan is set forth in Section 5.29.10. **Prepaid calling cards if approved and utilized must be available through the facility commissary.**

☑ **SECURUS has read and will comply.**

Prepaid for Friends and Family

Prepaid Accounts allow the end user complete control of his or her account. The customer can deposit any amount of money into the account and can monitor the amount of money s/he wishes to spend on collect calls from the prison.

Alternate billing options are presented to customer as the solution for call completion, such as Prepayment, or Direct Billing for Special Accounts (bail bonding companies, attorneys, public defenders, etc).

With prepayment, the customer is asked to submit payment to establish Prepaid Account. Payment options are:

- **Western Union Quick Collect**
- **Visa, MasterCard by phone**
- **Check by phone**
- **Money Order, Cashier's check by US Mail**

The customer must maintain a positive balance in account to avoid line restriction. The customer will receive an automated courtesy call when account balance reaches $20.

"This is Correctional Billing Services. This courtesy call is being made to advise you that the balance in your prepaid account is $20 or less. To prevent any interruption in your service, please forward additional payment, or call Correctional Billing Services at 800-844-6591. Again, that number is 800-844-6591. Thank you."

The end user can call into the Correctional Billing Services' automated system to access account status at any time, and can also talk to a live operator for assistance.

Prepaid Debit
SECURUS' prepaid debit option allows inmates to pay for the calls they make from a correctional facility, including international calls, with funds from their trust account transferred to a telephone pre-pay account.

Facilities utilizing the SECURUS system have complete administrative control over this prepaid option, including establishing the prepaid accounts, applying funds to those accounts, managing reporting functions and issuing refunds where appropriate.

Each prepaid debit account utilizes a PIN to ensure the inmate's account is properly secured and no one else can charge calls to that account. The account balance is announced at the beginning of each prepaid debit call, and the call will only be placed if the account has sufficient funds to pay for at least a one minute call.

5.29.2 At the beginning of the contract term, the prepaid, PIN-controlled mode shall be fully implemented at all DOC institutions listed in Table One. It is the intention of DOC to implement the ITS in a prepaid mode for all 50 states, United States territories and international countries.

☑ **SECURUS has read and will comply.**

5.29.3 The proposed ITS shall process prepaid or collect calls depending on the choice made by the inmate caller or automated equipment. When placing a call, the inmate will be prompted, in advance, of insufficient funds on the account. The ITS shall confirm that funds are available in the pre-paid account after the telephone number and PIN are dialed by the inmate, but prior to placing the call.

☑ **SECURUS has read and will comply.**

5.29.4 In order to utilize the features of the prepaid calling plan, the ITS system must be configured to use system PINS for phone calls. The ITS prompts for this information after capturing the dialed digits for each call. The ITS system should use both the called number and the PIN to make prepaid call decisions. The PIN and telephone number identifies the prepaid account that must be checked for a sufficient balance. In order to insure appropriate coverage of prepaid call charges, the ITS system should freeze sufficient number of minutes allowed by the duration controls and the prepaid call rates which are mileage banded, date, and time-of- day sensitive.

Money is frozen so that no other withdrawals may be made on that account while a call is in session. If the account balance is less than the amount needed to cover the maximum allowed call duration, the call is processed either as a prepaid call, but only for the length of time allowed by the existing balance or processed as a collect call.

☑ **SECURUS has read and will comply.**

SECURUS employs the most sophisticated intelligent validation network in the industry. As a real-time validation system, each dialed number is thoroughly analyzed before the call is allowed to process. This includes determining payment options, balance of the account, if the area code and exchange are valid, checking the number against any restrictions such as customer requested blocks, and verifying type of phone service through the national Line Information Data Base (LIDB). Once the dialed number passes all these tests it will be dialed by the system.

The SECURUS Secure Call Platform (SCP) offers standard calling cards and an additional option for automated card-less debit calling that are linked to the inmate PIN. Optionally, the DOC can create a separate debit calling account through which the inmate purchases a set amount that is then resident in the inmate telephone system (SCP Debit). All information regarding debit becomes part of the profile for the inmate. If the inmate is transferred, all profile information including debit balance is also transferred with the inmate.

5.29.5 The proposed ITS must provide for true "answer supervision" for the debiting of prepaid charges. Debiting shall begin when the call is answered by the called party and shall terminate when either the inmate or the called party hangs up.

☑ **SECURUS has read and will comply.**

5.29.6 The Offeror shall provide the prepaid call services required in this RFP through the use of an automated operator. An inmate shall never be connected to a "live" operator.

☑ **SECURUS has read and will comply.**

5.29.7 The Offeror must describe the following functionality when the ITS system is operating in a prepaid mode:

A. Prompts inmate callers of:

(1) The dialed number is not on the inmate's approved calling list.

☑ **SECURUS has read and will comply.**

The Secure Call Platform will prompt inmate callers in the prepaid mode if the dialed number is not on the inmate's approved calling list.

(2) To select the pre-paid or collect option after the phone number and PIN is keyed in, unless automated equipment handles this function.

☑ **SECURUS has read and will comply.**

The Secure Call Platform will prompt the inmate to select the pre-paid or collect option after the phone number and PIN is keyed in. The feature can be programmed according to the Alaska DOC's needs.

a. The call being terminated because of insufficient funds in the pre-paid account.

☑ **SECURUS has read and will comply.**

The account balance is announced at the beginning of each prepaid debit call, and the call will only be placed if the account has sufficient funds to pay for at least a one minute call.

D. Checks account balance to determine whether sufficient funds exist to place the call.

☑ **SECURUS has read and will comply.**

SECURUS' prepaid debit option allows inmates to pay for the calls they make from a correctional facility, including international calls, with funds from their trust account transferred to a telephone pre-pay account.

Facilities utilizing the SECURUS system have complete administrative control over this prepaid option, including establishing the prepaid accounts, applying funds to those accounts, managing reporting functions and issuing refunds where appropriate.

Each prepaid debit account utilizes a PIN to ensure the inmate's account is properly secured and no one else can charge calls to that account. The account balance is announced at the beginning of each prepaid debit call, and the call will only be placed if the account has sufficient funds to pay for at least a one minute call.

E. Sets the minimum and maximum call durations.

☑ **SECURUS has read and will comply.**

With SECURUS' calling platform, inmate call duration is completely programmable and may be limited to a specific time interval, e.g. 15 minutes per call. The time limit may be changed for each active line, individual inmates, and/or the entire system. Additionally, the Alaska DOC can choose to limit the number of calls per day or week, hours during

which calls can be made, and the type of calls that can be made during each time period.

A verbal warning can be given at three (3) minutes, one (1) minute, and thirty (30) seconds before the end of the programmed time interval, indicating that the call will be terminated. This feature is also programmable. Both the inmate and the called party are notified of call termination by voice prompting at one minute prior to the end of the call's pre-programmed time limit. By assigning a different Class of Service, call termination notification may be disengaged for specific numbers such as attorney's numbers, public defenders, etc. All call records contain a 'reason for termination' code that indicates why a call ended.

E. Allows or restricts calls based on standard call controls such as PIN, called number, phone used, and time of day.

☑ **SECURUS has read and will comply.**

Many restrictions may be tagged to any PIN or telephone number associated with a PIN.

Examples of restrictions are:

- **Time of day and/or days of week that a number may be called**
- **Maximum duration of a call for that number and/or PIN**
- **Maximum number of calls to that number or from that PIN per day/week/month/amount, etc.**
- **Allowed telephone numbers**
- **Phone used**

When restrictions are imposed, they are automatically managed by the calling platform.

5.29.8 The Offeror's Inmate Class of Service prepaid call **rates** charged to the inmate, within Alaska, regulated by the RCA, shall not exceed tariff per minute rates and tariff per call surcharges, applicable to local, intrastate/intraLATA toll and intrastate/interLATA calls originating from DOC facilities collectively, including surcharges. The called party will pay a per call surcharge regardless of the duration of the call, in addition to specified per minute rates that vary based upon the type of call. The intrastate/intraLATA per minute rates are mileage banded, date, and time-of-day-sensitive. The Offeror's Intrastate Tariff Rates shall remain fixed for the term of the Contract and not be changed without the DOC's written consent.

☑ **SECURUS has read and will comply.**

5.29.9 The Offeror's rates charged to the called party for **prepaid** calls outside of Alaska, regulated by the FCC, shall not exceed the tariff per minute rate for prepaid long distance calls and shall not exceed the surcharge rate for Inmate Class of Service. The Offeror shall provide its interstate per minute rate and surcharge. The Offeror's interstate tariff rate and surcharge shall remain fixed for the term of the Contract and not be changed without the DOC's written consent.

☑ **SECURUS has read and will comply.**

5.29.10 The Offeror shall provide a percentage of the gross call cost for all answered prepaid calls as a monthly commission fee to DOC. The monthly commission percentage paid to DOC shall not be less than 50% of the gross call cost for all answered prepaid calls. The Offeror shall not deduct fraudulent, un-collectible or un-billable calls, Local Exchange Carrier (LEC) access, LEC or long distance usage, maintenance or any costs of running the ITS, from the gross call cost for all answered prepaid calls prior to applying the commission percentage rate for DOC. In other words, the commission percentage rate shall be based on gross call cost including per call surcharges and per minute charges, not the net after expenses.

AMENDMENT NUMBER ONE:

The following changes/additions are required:

Change Section 5.29.10 of the RFP to read:

5.29.10 The Offeror shall provide a percentage of the gross call cost for all answered prepaid calls as a monthly commission fee to DOC. The Offeror shall not deduct fraudulent, un-collectible or un-billable calls, Local Exchange Carrier (LEC) access, LEC or long distance usage, maintenance or any costs of running the ITS, from the gross call cost for all answered prepaid calls prior to applying the commission percentage rate for DOC. In other words, the commission percentage rate shall be based on gross call cost including per call surcharges and per minute charges, not the net after expenses.

☑ **SECURUS has received and read the AMENDMENT NUMBER ONE changes and responded in the Cost Proposal as required.**

5.29.11 The Offeror's Rates for international calls shall be the current prevailing cost for international calls to the specific country being called.

☑ **SECURUS has read and will comply.**

5.29.12 A check for the commission amount, for the prepaid mode, shall be sent to DOC no later than 45 days after the close of the billing month. For example, a commission check for calls made during April shall be forwarded to DOC no later than June 15th. A summary report shall be provided with each commission check, that includes the following :

A. Total commission figure broken down by institution;

☑ **SECURUS has read and will comply.**

B. Listing of total minutes, total calls by institution;

☑ **SECURUS has read and will comply.**

C. Amount billed for services at each institution.

☑ **SECURUS has read and will comply.**

5.29.13 Inmates will get information on how to use the prepaid calling plan and how their family and friends can use it. The Contractor will provide information to the DOC outlining the policies and procedures of the prepaid calling plan, including but not limited to, a description of the features of the plan and instructions to families and friends as to how to set up the account. The DOC will then distribute this information to inmates. The Contractor shall work with the DOC to educate the inmates, friends, and families regarding the process for establishing a prepaid account and understanding the features of the plan. The Contractor will publish a "1-800" number for inquiries related to the prepaid calling plan. The Contractor's representatives will assist inmate family members and friends with payment questions and other customer service inquiries. The Contractor shall provide information regarding hours and days of operation of the customer service system on a 24 x 7 basis. All hours of operation shall be shown using Alaska time.

☑ **SECURUS has read and will comply.**

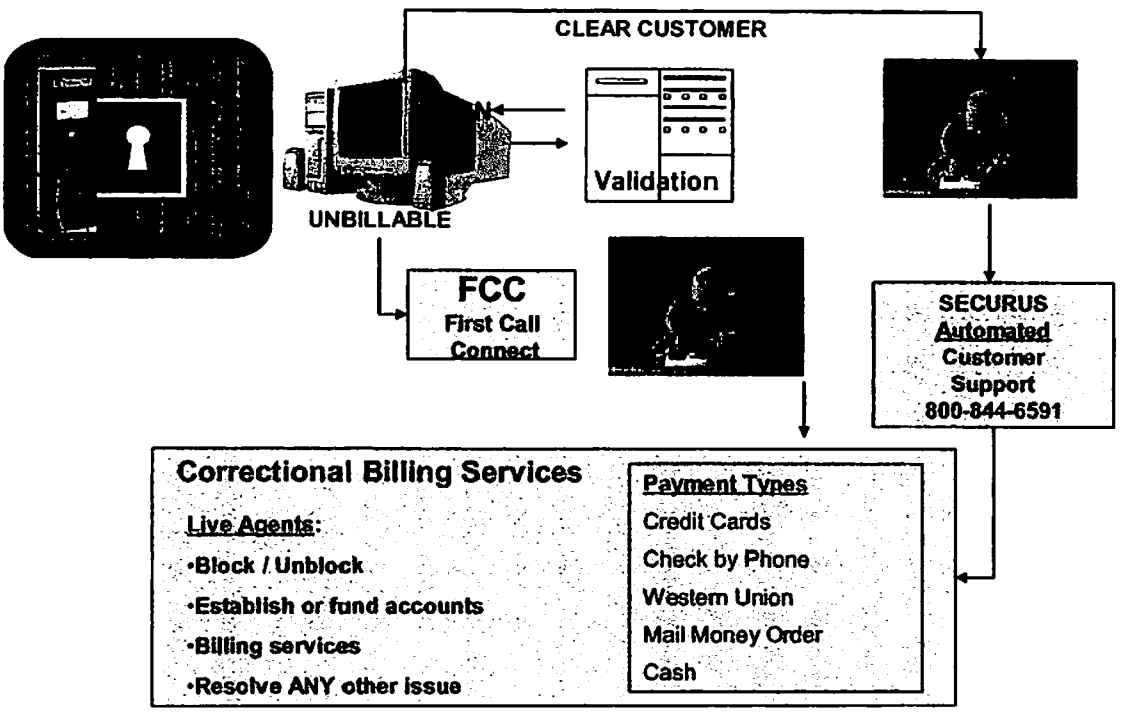
Prepaid for Friends and Family
Prepaid Accounts allow the end user complete control of his or her account. The customer can deposit any amount of money into the account and can monitor the amount of money s/he wishes to spend on collect calls from the prison.

Alternate billing options are presented to customer as the solution for call completion, such as Prepayment, or Direct Billing for Special Accounts (bail bonding companies, attorneys, public defenders, etc).

With prepayment, the customer is asked to submit payment to establish Prepaid Account. Payment options are:

- **Western Union Quick Collect**
- **Visa, MasterCard by phone**
- **Check by phone**
- **Money Order, Cashier's check by US Mail**

Below is an illustration of CBS process diagram.



The customer must maintain a positive balance in account to avoid line restriction. The customer will receive an automated courtesy call when account balance reaches $20.

> ***"This is Correctional Billing Services. This courtesy call is being made to advise you that the balance in your prepaid account is $20 or less. To prevent any interruption in your service, please forward additional payment, or call Correctional Billing Services at 800-844-6591. Again, that number is 800-844-6591. Thank you."***

The end user can call into the Correctional Billing Services' automated system to access account status at any time, and can also talk to a live operator for assistance.

Prepaid Debit

SECURUS' prepaid debit option allows inmates to pay for the calls they make from a correctional facility, including international calls, with funds from their trust account transferred to a telephone pre-pay account.

Facilities utilizing the SECURUS system have complete administrative control over this prepaid option, including establishing the prepaid accounts, applying funds to those accounts, managing reporting functions and issuing refunds where appropriate.

Each prepaid debit account utilizes a PIN to ensure the inmate's account is properly secured and no one else can charge calls to that account. The account balance is announced at the beginning of each prepaid debit call, and the call will only be placed if the account has sufficient funds to pay for at least a one minute call.

Friends and Family Assistance
SECURUS will provide both web-based and telephone-based access to family and friends for services including complaint resolution, call refunds, and number blocking/unblocking. Inmates' family and friends' concerns related to the Inmate Telephone Service will be handled by 400 professionals of the Correctional Billing Services (CBS), the largest Customer Care Center in the inmate calling industry. CBS is a division of SECURUS, created specifically to address billing, call blocking and any other concerns inmates and their families and friends might have. This division is also responsible for maximizing collect call completion and improving inmates' and their families and friends' communication. CBS is available to the inmates' friends and families 24 hours a day, 7 days a week through a call center (7days a week) or internet support applications (24 hours per day and 7 days a week).

SECURUS will also provide a brochure that the Alaska DOC can distribute to inmates with instructions on how friends and families can set up prepaid accounts.

Please refer to *Attachment M – Prepaid Calling Cards.*

5.30
Phase Out Plan

The Proposal shall describe a plan for a phase-out situation at the expiration or termination of the Contract term should the Offeror not be selected for the next contract to provide an ITS to DOC. Upon the expiration or termination of the Contract, should DOC award any succeeding contract for inmate telephone service to a vendor other than Offeror-Contractor, Offeror- Contractor agrees to cooperate fully and in all respects with the DOC, and the new contracted vendor in accomplishing an efficient and effective transfer of responsibilities.

☑ **SECURUS has read and will comply.**

It is SECURUS' standard practice to work closely with the customer and new vendor enforcing a smooth transition from our service to another, including but not limited to the existing PIN/PAN information to the new provider in a multitude of file formats. SECURUS understands that maximum uptime of communications is important to the facility and residents of the facility.

Installation of individual telephone sets is the most time consuming task during a transition and SECURUS allows purchasing of existing sets in place or if all new equipment is required, SECURUS will permit the new vendor to remove existing sets while installing their own.

Provisioned services from Local Exchange Carriers will remain active until all services for a facility have been replaced with the new vendor's services. Additionally all cable termination blocks installed by SECURUS will be clearly labeled and considered the property of the Alaska DOC providing a clear demarcation point for the new vendor.

5.31
Installation of the ITS Equipment and Software

5.31.1 Installation shall conform to the applicable Alaska Building Code, National Electric Code (NEC) and all other applicable national, state, and local codes and with accepted telecommunications' industry standards.

☑ **SECURUS has read and will comply.**

5.31.2 Where components, cables, cabinets, etc. are mounted on walls, ceilings, etc., suitable anchors shall be used, so that if any one hanger should fail, the device will remain securely in place.

☑ **SECURUS has read and will comply.**

5.31.3 Unless otherwise noted, all cable and components shall be supported by the building structure. Cables shall not be fastened to or lay on, a suspended ceiling. Cables shall not be fastened to the support wires of suspended ceilings, electrical conduits, or any mechanical or plumbing system pipe or other equipment.

☑ **SECURUS has read and will comply.**

5.31.4 All manufacturers' specifications and recommendations shall be strictly adhered to. Cable pulling tension and bend radii are critical because improper handling will cause physical abnormalities that will cause signal degradation.

☑ **SECURUS has read and will comply.**

5.31.5 The Offeror shall re-use existing station cabling installed at each DOC institution for the Inmate Station Equipment (Telephones). In cases where existing cabling cannot be used, the Offeror shall install new station cabling (Category 5E minimum) at no cost to DOC. Any new cabling shall include wall plate, cross connection, patch cords, etc., as required by the DOC.

☑ **SECURUS has read and will comply.**

5.31.6 The Offeror shall obtain DOC's permission, in writing, before proceeding with any work that requires cutting into or through girders, beams, concrete or tile floors, partitions, or ceilings, or any work that may impair fireproofing or moisture proofing, or potentially cause any structural damage. DOC does not anticipate that such work will be required to install the ITS equipment.

☑ **SECURUS has read and will comply.**

5.31.7 The Offeror shall protect all building components, finishes and equipment from damage and, if so damaged, the Offeror shall be responsible for any needed repairs or replacements, to the satisfaction of DOC.

☑ **SECURUS has read and will comply.**

5.31.8 The Offeror shall always keep the work site free from accumulation of waste materials and/or rubbish resulting from delivery of services. Offeror shall keep the site at least broom clean. Upon completion of installation at the work site, Offeror shall ensure that all of Offeror's tools, construction equipment, machinery, temporary structures; surplus/waste materials and rubbish are removed from the worksite.

☑ **SECURUS has read and will comply.**

5.31.9 Exposed wiring, wire mold or other surface mounted raceway shall not be permitted in finished areas unless pre-approved by DOC.

☑ **SECURUS has read and will comply.**

5.31.10 The Offeror shall provide all necessary labor, equipment and accessories to complete the installation work in a satisfactory manner.

☑ **SECURUS has read and will comply.**

5.31.11 The Offeror shall ensure that all of its work and materials shall comply with all local, county, state and federal laws, ordinances and regulations as well as any direction of inspectors appointed by proper authorities having jurisdiction at each DOC facility.

☑ **SECURUS has read and will comply.**

5.31.12 The Offeror shall acquire all necessary permits, etc. Should violation of Codes occur relating to this ITS, the Offeror shall correct the situation at no cost to DOC.

☑ **SECURUS has read and will comply.**

5.31.13 The Offeror shall conduct all work in harmony with other trades.

☑ **SECURUS has read and will comply.**

5.32
Wiring Standard

5.32.1 Any additional wiring work that is done shall be performed in accordance with the manufacturers' published standards and guidelines for a premise distribution system. The purpose is to establish the highest level of end-to-end capability and to prepare for future requirements.

☑ **SECURUS has read and will comply.**

5.32.2 Offeror shall follow manufacturers' wiring standards for cross-connect activities and any additional wiring that may be required throughout the building.

☑ **SECURUS has read and will comply.**

5.32.3 The Offeror is responsible for cross-connecting new systems to existing wiring schemes. Offeror should not assume that existing facility wiring is properly labeled and identified.

☑ **SECURUS has read and will comply.**

5.32.4 Offerors shall assume that there will be some changes to current station arrangements.

☑ **SECURUS has read and will comply.**

5.32 5 Grounding and bonding shall meet or exceed EINIA-607,

☑ **SECURUS has read and will comply.**

5.32.6 Additional telephone station wiring shall be twisted pair, 24 gauge, Category 5E, and shall be UL listed CMP, and shall conform to accepted industry, FCC and NEC Standards as applicable to size, color code, insulation, etc. All Offeror installed wiring shall be new.

☑ **SECURUS has read and will comply.**

5.32.7 Cable connections, splicing and termination shall be done in accordance with accepted industry practices and manufacturer's instructions.

☑ **SECURUS has read and will comply.**

5.32.8 All supporting devices for the cabling must not pinch, bind, crimp, or in any other manner cause the physical or performance characteristic alterations of the cables.

☑ **SECURUS has read and will comply.**

5.32.9 The Offeror shall be responsible for all costs associated with the testing of wiring, both new and old, in preparation for the implementation of the new ITS.

☑ **SECURUS has read and will comply.**

5.32.10 The Offeror shall be responsible for assuring that existing station wiring will not adversely affect the performance of the Offeror's equipment or subsystems and that distribution to user terminals will meet manufacturers and the DOC requirements.

☑ **SECURUS has read and will comply.**

5.32.11 The Offeror shall work with the DOC to determine the exact times when Inmate Station Equipment (Telephones) can be replaced to reduce "down time".

☑ **SECURUS has read and will comply.**

5.33
Patching and Painting

Offeror is responsible for restoring damaged walls, ceilings, and/or wall coverings to their original condition.

5.33.1 The quality of workmanship shall be "Type 1 - Recommended," as set forth in the latest edition of the Painting Specifications of the Painting and Decorating Contractors of America,

☑ **SECURUS has read and will comply.**

5.33.2. The quality of patching shall maintain the same fire rating as the original wall or ceiling covering.

☑ **SECURUS has read and will comply.**

5.33.3 Cutting and patching requirements shall be submitted to the DOC project representative for their approval.

☑ **SECURUS has read and will comply.**

5.34
Fire Stopping and Smoke Seals

Fire stopping includes, but is not limited to, openings in fire-rated floors and walls for cables, conduits and trays. Fire stopping materials shall conform to ratings as required by local and state building codes and as tested by nationally accepted test agencies per ASTM E814 and UL 1479 fire tests.

5.34.1 Fire ratings shall be a minimum of one (1) hour but not less than the fire resistance of the floor or wall being penetrated.

☑ **SECURUS has read and will comply.**

5.34.2 Codes and Standards for fire stopping materials include:

ASTM E814

UL 1479

NFPA 101-88. 6-2/2/5 and 6-2.2.8

☑ **SECURUS has read and will comply.**

5.34.3 Installation shall conform to manufacturer's printed instructions for installation.

☑ **SECURUS has read and will comply.**

5.34.4 Fire stop materials shall be non-combustible silicone elastomer sealant having a UL classification as a "fill, void or cavity material."

☑ **SECURUS has read and will comply.**

5.34.5 The Offeror shall submit manufacturer's product data, specifications, and installation instructions to the DOC Project Representative for review and approval prior to making any penetrations.

☑ **SECURUS has read and will comply.**

5.34.6 All penetrations and accompanying fire stopping shall be documented in writing by the Offeror. Such records shall include objects penetrated, characteristics of the penetration, and location,

☑ **SECURUS has read and will comply.**

5.34.7 DOC staff and applicable Code authorities shall examine fire stops prior to closing out work.

☑ **SECURUS has read and will comply.**

5.34.8 Fire stopping of new penetrations shall occur by the end of each working day.

☑ **SECURUS has read and will comply.**

5.35
Security

The work comprising this ITS shall be performed at DOC institutions listed in Table One. The Offeror and subcontractors shall comply with the following special working conditions:

5.35.1 Be cleared for security access by DOC. Offeror shall submit a list of names of all persons expected to be on the work site. The completed list shall be submitted, for approval, to the DOC prior to any person's appearance at the work site. See attachment 10, Security Information Sheet.

☑ **SECURUS has read and will comply.**

5.35.2 Daily check-in with DOC security and follow all DOC security rules.

☑ **SECURUS has read and will comply.**

5.36
Safety

5.36.1 Offeror shall comply with federal, state, municipal, and OSHA laws, rules, regulations, and code requirements.

☑ **SECURUS has read and will comply.**

5.36.2 Offeror shall be responsible for initiating, maintaining, and supervising all safety precautions and programs in connection with performing Contract services. Offeror shall take all reasonable precautions for safety of, and shall provide all reasonable protection to prevent damage, injury, or loss to the following: (A) all employees providing service and other persons who may be affected thereby; (B) all materials and equipment to be used in providing the services; and (C) other property at the site or adjacent thereto.

☑ **SECURUS has read and will comply.**

5.36.3 Offeror shall ensure that required fire-fighting apparatuses are accessible at all times. Flammable materials shall be kept in suitable places outside the DOC institution.

☑ **SECURUS has read and will comply.**

5.36.4 The Offeror shall comply with all DOC requirements for facility access including, but not limited to, tool control, background checks and dress code,

☑ **SECURUS has read and will comply.**

5.37
Problem Notification

If the Contractor becomes aware of possible problems that could result in delay in completion of the ITS system or schedule then immediately notify the designated DOC project representative by telephone, with written confirmation within 72 hours, giving the cause and probable effect, and recommendations for corrective action. Failure to promptly notify DOC may be a basis for determining Contractor's negligence in an otherwise excusable delay. Possible delay problems shall not be interpreted as relieving the Contractor from contractual responsibilities.

☑ **SECURUS has read and will comply.**

5.38
Delivery

DOC may delay any delivery to a mutually agreeable time. All deliveries shall be FOB destination. The Offeror shall be on-site to receive all deliveries.

☑ **SECURUS has read and will comply.**

5.39
Work Schedule

The successful contractor will be required to submit their filing for RCA certification within 30 days of contract award.

☑ **SECURUS has read and will comply with the understanding that upon contract award, required filings for local collect calling will be submitted**

immediately with the Regulatory Commission of Alaska. Delays beyond the control of SECURUS do to RCA's untimely approval of applicable tariff's should not be considered as a failure to perform.

The systems must be installed and fully operational within 120 days of RCA certification of the successful contractor. The successful contractor must comply with all RCA requirements.

☑ SECURUS has read and will comply.

Experience and Qualifications

Staff Qualifications – A current resume/vitae of education, training and experience for each individual (contractors, contract staff, subcontractors, and volunteers) who will be providing direct treatment services must be included with the offeror's proposal. If the offeror proposes to utilize a subcontractor for the provision of services, a letter of commitment and current resume/vitae from each proposed subcontractor must also be included with the offeror's proposal. (See Section 1.14 for more information on subcontracting.)

Resumes must include information that clearly delineates the qualifications, training, and experience of each individual who has been identified to provide services under the terms of the contract. (Copies of current state licenses and certifications must also be included, as appropriate. See Section 6.03[b]).

☑ **SECURUS has read and will comply.**

SECURUS has an organizational structure designed to provide efficient delivery of services and products to our customers. The following are unique departments and their primary responsibility in delivering outstanding service to our customers:

Department	Role
Field Operations	Maintenance of Equipment and Networks
Engineering	Designs Customer Specific Systems
Installation	Installs New Systems
Service Center	Trouble Reporting and Resolution
Network Operations Center	Network Monitoring and Trouble Resolution
Customer Billing Services	Account interface for Friends and Families
Administrative Services	Provides Administrative Assistance to Facilities
Billing Operations	Manages the Billing/Account Validation Process
Product Management	Product Lifecycle Management
Applications Development	Creation of Software and Telephony Programs
Quality Assurance	Application and hardware testing
Research and Development	Scientific Innovation Applied to Products
Accounting and Finance	Financial Integrity
Human Resources	Attracting and Retaining High Quality People
Purchasing	Supplier Identification and Order Fulfillment
Legal	Contract and Corporate Compliance
Regulatory	Compliance with local, state and federal regulations
Customer Satisfaction	Obtains Customer Feedback via Surveys
Sales	Customer Communications
Marketing	Product and Corporate Promotion

The most important aspect of our organization structure as presented below is that each of these departments is committed to providing the administrative structure that interfaces with our accounts. The key person in our administrative structure will be Kevin Collins, the Account Manger for your account. The Account Manager is your single point of contact for all issues relating to services and products provided by SECURUS. For the

Alaska DOC, the Account Manager will be dedicated to your account and will be assisted by Ken Rose, Regional Service Manager, and dedicated to provisions of services to the Alaska DOC. From an administrative perspective, the Alaska DOC will also be in contact with our service center, 24 hours a day, 7 days a week, to report specific problems at your sites.

SECURUS has provided brief BIOS for each of our key personnel below. For detailed resumes, please refer to *Attachment J – SECURUS Key Personnel Resumes.*

Kevin J. Collins, Senior Account Executive
SECURUS Technologies DOC Team
Kevin Collins has been with SECURUS Technologies in various management capacities for eleven years and has been involved in the telecommunications industry for over 22 years. As Senior Account Executive for the SECURUS DOC team his responsibilities are establishing the business relationships with State Department of Corrections and managing the Canadian Corrections Market with strategic partners.

Further responsibilities are interfacing with various account teams, product teams and Industry consultants to develop creative solutions. His past experiences include the role as Regional Vice President Prison Market. His role included the account management of several Regional Bell Operating Companies, State Department of Corrections market, and the Canadian Corrections market. His various past responsibilities included the management of the T-NETIX account management team for the Midwest and Qwest Communications territory. The Canadian Criminal Justice relationship was initiated in February 2000 as the Canadian corrections market opportunity emerged with TELUS Communications.

Prior to joining T-NETIX, Inc. Mr. Collins was in sales management in the telecom industry managing a $100M+ annual revenue stream in major account markets including IBM, Hewlett- Packard, Chevron, Lockheed Martin, Lucent, and Exxon.

Ross Preston, Account Executive
Ross Preston has over 24 years experience in the telecommunications industry. He has held management positions with MCI Telecommunications, Qwest Communications and Verizon Business. The past 12 years of his career has been spent serving the Government Markets sector for a variety large communications contracts. Those contracts included; inmate telecommunication services, voice, video and data as well as application based services. While with MCI Telecommunications Ross was the company liaison with direct responsibility for the partnership with the DOC's satisfaction. Ross has overseen inmate telecommunications contracts for the State of Florida, Arkansas and Louisiana.

Andy Fall, Former Territory Manager

Andy Fall is the current Account Manager for SECURUS Technologies serving the Alaska DOC and has acted in that capacity since December 2004. Andy currently provides Account Management for facilities in Idaho, Oregon and Washington as well.

Andy has over 10 years experience in sales and sales support of Inmate Telephone Systems to City, County, State and Special Jurisdictions and over 20 years experience in sales and sales support of products and services to the Corrections Industry including commissary, trust fund software and identification biometrics

Andy holds an undergraduate degree from Whittier College and a graduate degree from Pepperdine University.

Andy is based in Portland, Oregon.

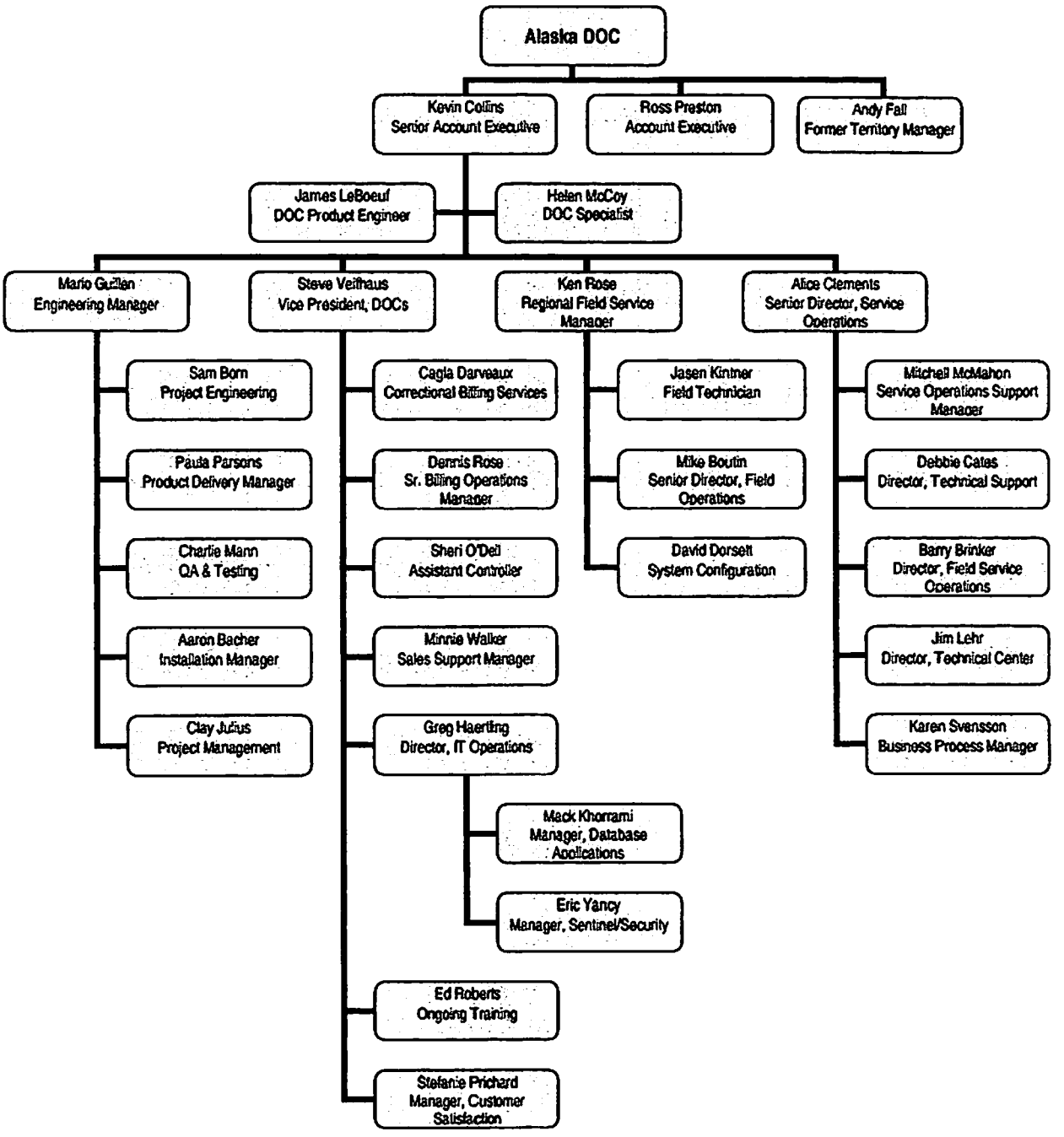
Ken Rose, Regional Field Service Manager
Ken is currently responsible for all Field Service Technicians in WA, AK, OR, NV, CA, & AZ. He will be the first point of contact for any escalation issues that may arise. Ken has over 26 years experience in the telecommunication field, with the last 8 years in the inmate industry. He holds a Masters degree in Computer Information.

James LeBoeuf, DOC Product Engineer
James has supported inmate systems and correctional facility accounts for over 17 years in Operations Management and Technical Sales. He has been directly involved with Installation and Maintenance of 300+ correctional facilities and indirectly involved as team management for 1000+ facilities throughout the Continental US and Alaska.

Helen McCoy, DOC Sales Specialist
Helen has more than 30 years experience in telecommunications customer service, resolving service concerns/issues to ensure customer satisfaction. During her time with SECURUS, she has been responsible for coordination of system solutions including installation, maintenance and repair and has handled special long distance contracts for the Indianan Department of Corrections, Kansas Department of Corrections, and New Jersey Department of Corrections.

Jasen Kintner, Field Technician
Jasen has sixteen years combined telecommunications experience with the United States Army, General Communications, Inc., Communications Consultants, Inc., and SECURUS Technologies, Inc. He is a four-time Army medal awardee for outstanding job performance who prides himself on adapting readily to difficult situations and working hard to produce a favorable solution. His experience includes developing a course of

instruction for a company of 185 people which resulted in improved and enhanced communications in fixed, mobile, and remote site locations.



Experience Providing Services – (Distinguish between an agency or individual managing or administering services as opposed to direct services provision.) The offeror must indicate prior experience in administering the services required under this RFP, or similar services, including any experience in providing services within correctional environments and/or to correctional clientele. At a minimum, offerors should address the following in their submitted proposals:

☑ **SECURUS has read and will comply.**

Include a description of similar services provided and dates;

Include reference names and phone numbers that can provide confirmation of services rendered.

☑ **SECURUS has read and will comply.**

References

North Dakota DOC
Tim Schuetzle, Director of Prisons
3100 Railroad Ave
Bismarck, ND 58501
(701) 328-6111
701.328.6640 (Fax)
Tschuetz@state.nd.us

North Dakota DOC has 1,400 inmates in 3 facilities with approximately 80 inmate telephones. All DOC facilities installed our call management systems since 1995. Current systems provide for collect and prepaid calling services, integrated recording, and Web managed applications.

Indiana DOC
Office of Information Technology
Greg Tuttle, Telecom Manager
Technology Services Division
302 West Washington
Indianapolis, IN 46204-2738
317.232.6933
317/232-5865 (Fax)
GTuttle@tsd.doc.state.in.us

Indiana DOC has 21,500 inmates in 30 facilities served by 1168 phones. State of Indiana awarded a four year long distance service contract with two year options for the Department of Corrections to T-NETIX a subsidiary of SECURUS technologies in September 2001. All DOC institutions have been utilizing SECURUS call management systems with recording capability since 1995.

Maryland DOC
Dayena M. Corcoran
Asst. Warden
Maryland DPSCS
MCI Women's
7943 Brockbridge Rd.
Jessup, MD 20794
(410)379-3803
In a very rate conscious State of Maryland (ADP 26,750, director provider for the last 3 yrs., call platform provider since 1994) SECURUS was able to substantially reduce costs to inmates and their families and still provide outstanding investigative capabilities and service, with no service interruptions.

TELUS Communications DOC
David Fowler, Director
3202-25 Avenue SW
Calgary, Alberta
Canada T3E0K6
(403) 530-4512
(877) 711-0111

TELUS Communications utilizes a SECURUS Technologies centralized call processing networked based system for all British Columbia and Alberta Provincial correctional facilities installed in April 2001. Platform provides for collect and prepaid calling services, integrated recording, Web managed applications, and Voice verification application.

Governing Policies – if applicable, include a copy.

☑ **SECURUS has read and will comply.**

A sample Service Schedule and Master Services Agreement are included in *Attachment K – SECURUS MSA and Service Schedule.*

Litigation History – Offeror must include a summary of all litigation (including bankruptcy cases) associated with providing the same services, or services similar to those required in this RFP. Include past five years and present litigation in which the offeror (and any person in this offeror's current administration who will be responsible for the administration or operations related to providing these services) has been named a party, including state jurisdiction, case number, and final disposition. Litigation of personal issues not germane to the services herein (i.e., automobile not related to substance abuse, divorce, child custody or support) is not required.

☑ **SECURUS has read and will comply.**

In response to the request for a statement from the Offeror, which in our case is both Evercom and SECURUS (referenced collectively as the "Companies"), explaining any lawsuits specifically associated with providing the same services, or services similar to those of this RFP, which were filed within the last five years, the Companies have, from time to time, been subject to various legal proceedings and claims that arise in the ordinary course of business operations, including, suits brought by prisoners or their family members and by our competitors involving patent matters. The Companies believe that the ultimate disposition of the pending litigation will not have a material impact on its financial condition or its ability to perform under the proposed contract. With respect to the Companies' material litigation, a list can be found on a regular basis in SECURUS' Annual Report publicly filed with the U.S. Securities and Exchange Commission. The cases in the Annual Report that involve Evercom or SECURUS have been explained in detail below for easy reference.

Evercom was recently dismissed from a lawsuit in the Superior Court for the State of California in and for the County of Alameda, captioned *Elena Condes, Brian H. Getz, Bicka Barlow and Christopher Fank, on behalf of themselves and all others similarly situated v. Evercom Systems, Inc. et al,* Case No. 2002054255, filed on June 12, 2002. In *Condes*, Evercom, along with other inmate telecommunications providers, was named in this suit in which the plaintiffs have alleged that they were incorrectly charged for collect calls from a number of correctional facilities as a result of systematic defects in the inmate calling platforms of all the telecommunications provider defendants. Evercom executed a settlement agreement with plaintiffs in December 2005, and the court granted final approval of the settlement in 2006. Evercom did not admit to any wrongdoing and has vigorously denied each and every allegation in the case.

On February 2, 2006, Evercom was named in a putative class action in Florida federal court captioned *Kirsten Salb v. Evercom Systems, Inc., et al.*, filed In the United States District Court for the Southern District of Florida – Miami Division, Case No. 06-20290-civ-UNGARO-BENAGES/O'SULLIVAN. Evercom is alleged to have violated the Florida Deceptive and Unfair Trade Practices Act and other common law duties because of the alleged incorrect termination of inmate telephone calls. Plaintiff, who received calls from an inmate, seeks restitution and compensatory on behalf of a class of persons who receive inmate calls from Florida correctional sites that are served by Evercom's platforms. The court has recently administratively dismissed the case.

Moving to the cases involving patent matters, Evercom, Inc., Evercom Systems, Inc., Evercom Holdings, Inc., (referred to collectively as "Evercom") are named parties in the lawsuit captioned *TIP Systems, LLC and TIP Systems Holding Co., Inc. v. Phillips & Brooks/Gladwin, Inc., et al.*, Case No. H-04-371, filed September 24, 2004, which was filed in the United States District Court for the Southern District of Texas (Houston Division). In *TIP Systems*, Evercom, along with other inmate telecommunications providers, is alleged to have infringed on patents concerning "cord-free" or "hands-free" inmate phone technology. This lawsuit

against the Evercom defendants recently was dismissed on March 1, 2007, when the Evercom Defendant's motion for summary judgment was granted on the issue of non-infringement. This case is on appeal. The TIP Systems entities have also filed a lawsuit captioned *TIP Systems, LLC and TIP Systems Holding Co., Inc. v. SBC Operations, Inc., et. al.*, Case No. H06 0253, filed January 23, 2006, which was also filed in the Southern District of Texas. SECURUS Technologies, Inc. is a named party to the suit, which alleges substantially similar allegations concerning patent infringement claims for "cord-free" or "hands-free" inmate phone technology. SECURUS Technologies denies any wrongdoing and will vigorously defend each and every allegation in the case. This case is still pending and our company has filed a motion for summary judgment.

On November 9, 2005, SECURUS Technologies, Inc. filed suit in the District Court of Dallas County, Texas, Case No. 05-11374-M, against AGM Telecom Corporation and former employees of various Company affiliates, captioned *SECURUS Technologies, Inc. v. David McEvilly, George McNitt, Thomas Miller, Steven Capitano, Brian Dietert, and AGM Telecom Corporation*, alleging, among other things, breach of contract and misappropriation of trade secrets. In the lawsuit, various defendants have counterclaimed for alleged violations of the Texas Business & Commerce Code, for disparagement, defamation, and tortious interference. The court recently granted the motion of certain Defendants to compel arbitration of the matter. Case is currently set for non-jury trial on September 18, 2007. The Company denies any wrongdoing with respect to the alleged counterclaims and will vigorously defend each and every counterclaim asserted by defendants.

On October 4, 2006, Evercom Systems, Inc., filed suit in the U.S. Federal District Court for the Eastern District of Texas, Case No. 2-06cv-426-TJW, against (i) Global Tel*Link Corporation; (ii) AGM Telecom Corporation; and (iii) FSH Communications, LLC. for patent infringement of several patents related to the inmate correctional services and telecommunications industry by each such defendant. Discovery has commenced in this case.

Naturally, from time to time in providing services elsewhere throughout the country, minor invoice disputes or small claims cases arise in the ordinary course of business parties who are billed for inmate calls and these matters are successfully resolved either to the satisfaction of both parties or through affirmative relief granted by the court to dismiss claims lacking merit.

By this response, the Companies have used their best efforts to provide a thorough statement based upon records accessible to the Companies. The descriptions are intended to fully satisfy the request for a statement explaining the litigation of the Companies, while recognizing that certain outside persons having access to this publicly available document could use information for inappropriate purposes, unintended by the requesting party. If any additional

specifics are required related to matters described herein the Companies will certainly accommodate any such reasonable request.

Budget Narrative

Proposers are to include an explanation of how the costs were derived in sufficient detail to allow analysis of the logic, adequacy, and appropriateness of the offeror's proposed budget. (The proposal's budget narrative will be evaluated as part of Section 6.04[a].)

☑ **SECURUS has read and will comply.**

SECURUS will be providing service at NO COST to the Alaska DOC. SECURUS has built a business case and financial model that estimates the revenue associated with end user collect and prepaid calling charges and compares this revenue to cost of providing service. Under the terms of this contract, SECURUS will not charge the Alaska DOC for any of the SECURUS costs listed below.

- **A major cost component is the sharing of revenue (commission payment) with the Alaska DOC**
- **Bad debt**
- **Engineering**
- **Equipment costs for telephones, customer premise equipment, including equipment used for network services and call processing**
- **Installation and maintenance associated with this equipment**
- **Shipping charges**
- **Insurance and Bond fees**
- **Taxes**
- **Sales costs, including travel and expenses**
- **Personnel costs associated with field support services**
- **Personnel costs associated with call center customer services**
- **Toll free calling to customer service**
- **Line charges for access services**
- **Long distance telephone charges for network services**
- **Call validation services**
- **Billing and Collection charges**

As mentioned in previous responses, SECURUS has an industry leading position in the inmate telecommunications market. The competitive market requires that SECURUS provide high quality service at competitive end user rates with a competitive commission offering.

Personnel – The rates proposed must include all direct and indirect costs associated with performance of the services required in this RFP. Direct cost is the cost of the individual's time providing the direct service that includes, but is not limited to, personnel costs and fringe benefits. Indirect costs associated with the performance with this contract include but may not be limited to insurance, supplies, overhead, local travel, etc.

☑ **SECURUS has read and will comply.**

The cost of a technician per year is $ 78,000 per year. This includes both salary and fringe benefits cost for the employee. There is also a direct cost of travel of approximately $ 100 k per year. This includes meals, airfare, lodging and vehicle rental. We will also incur substantial indirect costs these include customer service, billing & collection, and selling, general and administrative costs.

Travel Expenses – Proposed compensation for travel, if applicable, (and in general for offerors who live outside the service area) for the purpose of providing services under Section Five of this RFP should be clearly stated in the budget narrative and cost proposed.

Offerors should clearly specify the number of trips that will be necessary (annually) to provide services as specified in their proposed Plan for Services. Provide as much detail as necessary to support any travel and related costs.

Compensation for travel, if proposed, may consist of lodging, meals, and travel expenditures for the purpose of providing services under this RFP. See Attachment #10 for travel reimbursement policy.

☑ **SECURUS has read and will comply.**

As the incumbent ITS provider we have not forwarded any requests for compensation for travel expenses. We believe this is all part of our doing business with the State. In answer to the question we have been to each site in 2007 as listed below:

	Preventive Maintenance	Handset Repairs	Misc Phone Issues	Installation - Additions and Moves	System and Network Issues
AK - ANCHORAGE JAIL	5	50	10	1	2
AK - ANVIL MT.	1	5	8		
AK - COOK INLET	3	33	17	1	5
AK - FAIRBANKS	1	26	17	1	3
AK - HILAND/MEADOW	3	12	10		5
AK - KETCHIKAN	1	12	7	1	1
AK - MATSU	3	8	13	1	
AK - PALMER	3	16	14	2	10
AK - POINT MACKENZIE	1		11	1	2
AK - SPRING CREEK	1	10	21	1	1

	Preventive Maintenance	Handset Repairs	Misc Phone Issues	Installation - Additions and Moves	System and Network Issues
AK - WILDWOOD	4	23	14		1
AK - YUKON-KUSKOKWIM	1	19	7		
AK - LEMON CREEK	1	30	10		1
Totals	28	244	159	9	31

This resulted in unreimbursed travel expenses as follows:

16 Flights	**$8600**
Lodging and Meals	**$470**
Other Transportation (ferry's/cabs)	**$96**
Mileage 19,723 miles @$0.345	**$8776**

Attachment B

SECURUS Executive Summary

SECURUS Technologies, Inc., providing services through its wholly owned subsidiary Evercom Systems, Inc., appreciates the opportunity to submit this proposal to the Alaska Department of Corrections for Inmate Telephone Systems. Your SECURUS account team has completely reviewed the requirements of the inmate telephone system and we are prepared to provide the Alaska DOC with a "turn key" state of the art technology driven inmate telephone system. Furthermore, SECURUS will provide at no cost to the state all call processing, monitoring and recording equipment, professional installation and ongoing maintenance for the term of the agreement.

Additionally, we believe that our response will go beyond the stated requirements by affording the Alaska DOC new revenue generating capabilities, superior investigative tools, more efficient use of correctional officers time and the ability to implement necessary inmate telephone system changes remotely.

Our company values, as demonstrated each day, include integrity, respect, and keeping commitments made to customers. The result is a company and a brand that you can trust and a company that has proudly served this industry since 1988 and the Alaska DOC since 1994.

The Alaska DOC is asking offerors to begin charging for local calls. SECURUS is pleased to announce that GCI will be a partner on our team and will be providing billing and collection services for local calling. GCI (NASDAQ: GNCMA) is an Alaska-based company providing voice, video and data communication services to residential, commercial and government customers. Founded in 1979, GCI introduced long-distance competition to Alaska and has since grown to be one of the nation's premier integrated telecommunication providers. The company employs 1,250 Alaskans and has a current revenue stream of $440 million.

We will be working closely with GCI in their efforts to obtain the required tariff and regulatory approvals from the Regulatory Commission of Alaska for local collect calling services. We applaud the Alaska DOC for implementing a policy that will minimize local calling fraud. This action will result in increased safety for the general public, corrections officers and inmates. With free local calling a high percentage of call recipients have likely subscribed to remote call forwarding (RCF) services. When RCF services are used, the Alaska DOC investigators are unable to determine name, phone number and address of the individual speaking with the inmate. Charging for local calls will help minimize this security risk. We encourage the Alaska DOC to be an active participant with SECURUS and GCI when we meet with the Regulatory Commission of Alaska seeking tariff approval to implement a more secure system.

Partnership with the Alaska DOC

We look forward to working with Alaska DOC through the life of this agreement and beyond. The partnership will be supported by dedicated resources, which will bring to bear the technology assets of SECURUS, in support of both inmate communications as well as the broader needs of Alaska DOC.

SECURUS has been your partner for over 10+ years, we understand the intricacies of the existing inmate telephone system.

SECURUS as the incumbent provider and through Jasen Kintner, our SECURUS Field Service Technician based in Anchorage, AK, has worked diligently to identify and deliver site specific support to insure maximum system reliability given the challenges of site locations and weather. This ongoing effort has included site visits throughout the year for maintenance, training and investigative support. We have established a preventative maintenance schedule that has included site visits at all Alaska DOC locations this past year, as well as moving various pieces of equipment and repairing over 244 phones as necessary.

SECURUS has worked closely with Sgt. Brett Bodner at the Palmer Correctional Facility, in eliminating calls to Cellular Phones from all of the Alaska DOC facilities, additionally by keeping the equipment running at near 100% uptime, we have assisted Sgt. Jim Bolgiano the Security Sergeant at the Anchorage Jail resulting in information being gathered that has resulted in numerous convictions.

Over the past several years system expansion and facility improvements have been coordinated at the site level directly with our local technician. In 2007 with the expansion that has taken place at the Matsu Correctional Facility, SECURUS able to work with the facility team headed by Mike Harbaugh & Sgt Larsen, resulting in the relocation of the equipment to a controlled room and increasing our system capacity to allow for additional telephone devices.

In 2006, SECURUS successfully coordinated system expansion as Alaska DOC expanded the Anchorage Correctional Complex, Lemon Creek Correctional Center, Fairbanks Correctional Center and Mat-su Pre-Trial Facility.

During 2005, field staff coordinated SECURUS efforts to successfully upgrade and deploy uniform inmate call control software to insure system wide compatibility and to insure investigators shared identical capabilities throughout all Alaska DOC sites.

On an ongoing basis we have virtually eliminated technical support escalation and reduced Called Party issues with Correctional Billing Services.

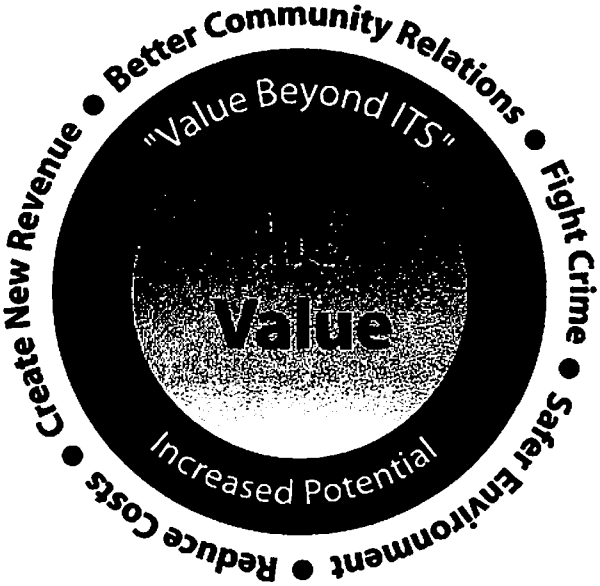
In this regard as it relates to Called Party inquiries and issues SECURUS will be ready and able to assist with the introduction of new local collect call rates. Anytime a rate structure is changed the billed to party will have questions. Those questions need to be answer by your partner not Alaska DOC personnel.

SECURUS approach this in several different ways. First, we will proactively approach customers who are currently accepting local calls and inquire if they would like to set up an account. Second, with the approval of the Alaska DOC, we will provide materials to the inmates and inmates friends and families with the new rate structure. Third, SECURUS Call Centers will be staffed appropriately to accept any customer inquires and be fully aware of the new rate structure.

The goal of this partnership is to provide a safer environment for inmates and correctional officers, improve productivity while returning commissions back to the Alaska DOC.

SECURUS Undertakes a New Direction for Customers

SECURUS Total Value Sphere



You will note in our responses that we now offer an even broader range of solutions to serve you. In fact, SECURUS has entirely redefined its mission to support your overall set of needs and challenges. Several years ago, fundamentally and powerfully supported by our excellence in ITS, we committed ourselves to offer solutions beyond just ITS. We have invested millions of dollars and nearly three years in people, skills, and applications in support of your goals beyond ITS. SECURUS Technologies has some 100 IT and product management professionals aimed at working with industry players and other technology companies to support your mission statement now and into the future. In other words, we are offering an expanded value proposition to the Alaska DOC beyond just excellence in ITS. A partnership founded on the tenets of your needs and our capabilities as represented by the diagram on the right.

Value Beyond ITS

It is therefore our commitment to not only address, thoroughly and completely, the inmate telephone system requirements contained within this RFP, but through a partnership with the Alaska DOC, help you achieve the department's overarching mission as quoted below:

Mission Statement

"The Alaska Department of Corrections enhances the safety of our communities. We provide secure confinement, reformative programs, and a process of supervised community reintegration."

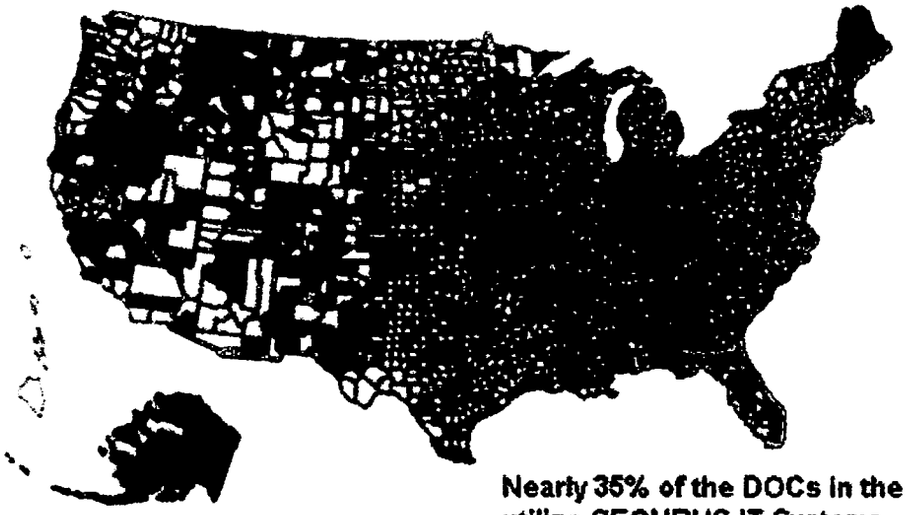
Corporate Financial Stability

H.I.G. Capital, a Miami-based private equity firm is the principal owner of SECURUS Technologies. H.I.G. Capital is a leading private equity and venture capital investment firm with more than $3 billion of equity capital and $5 billion in annual revenue currently under management. H.I.G. invests in management-led buyouts and recapitalizations of well-established, profitable, and well-managed manufacturing or service businesses, and in promising early-stage technology companies. The resources that H.I.G. brings to SECURUS allow us to continue our strong growth and customer service excellence.

Industry Experience

SECURUS possesses unrivaled experience and innovation in the provision of inmate calling combined with our first-hand knowledge of the challenges and obstacles faced by over 2,900 correctional facilities nationwide, thus allowing SECURUS to propose the optimum solution for the Alaska DOC.

- **Nationally, over 500,000 state DOC inmates in 17 state DOCs are using SECURUS calling platforms.**
- **More than 40 million local and long distance inmate call transactions are being processed each month by SECURUS across 52,000 lines.**
- **Over 400,000 Inmates in other facilities are using SECURUS calling platforms (this includes County, City, Military, Federal, Private Prisons, Community Centers and Halfway Houses).**



Nearly 35% of the DOCs in the U.S. utilize SECURUS IT Systems

******All DOCs using SECURUS' platforms whether on a subcontractor basis or a direct customer basis are outlined in red.***

Our vast customer base allows SECURUS to keep a finger on the pulse of the corrections industry allowing us to identify trends in inmate calling and adapt to a constantly evolving secure calling and investigative management industry.

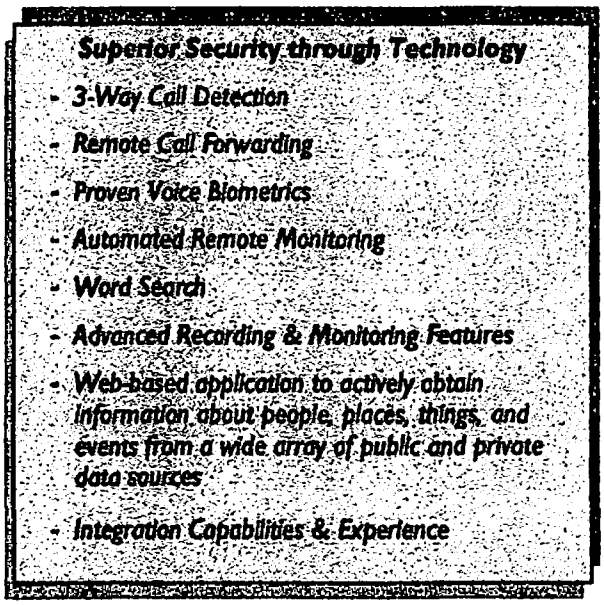
Investigative Tools

We offer leading edge crime fighting tools designed by and for investigators that provide visibility to activity within a single facility or all facilities across the State of Alaska. Additionally, we are driven to deliver automated, self-service applications to reduce your staff's involvement in mundane administrative tasks and enable them to concentrate on control and command functions.

A few examples of the many applications we have to meet your needs are:

- **Investigative Efficiencies:**
  - **3-Way call detection – we have 11 patents granted and three patents pending; industry leading precision and performance by a significant margin (detecting true 3-Way calls and eliminating false positives)**
  - **Remote call forwarding detection – proprietary process that proactively detects automatically forwarded calls**
  - **Advanced recording and monitoring – user-friendly, powerful, flexible recording and monitoring capabilities with immediate access to current and past recorded data**
  - **Covert Alert – enhances investigative efficiency by allowing secure monitoring of calls anywhere, anytime**

- Scan Patrol – exclusive SECURUS feature allows investigators to sample in-progress calls at a self-defined frequency
- ECHO – word search solution for correctional facilities
- SecureVoice – powerful voice biometric which authenticates the inmate's PIN



* Facial Recognition – human identification face shape analysis technology
* Electronic Dragnet – powerful, web-based investigative national data search application; we believe Electronic Dragnet would be a significant tool for your FACT unit to provide a system-wide approach to apprehend absconders
* Denotes optional application

This is all fundamentally enabled by our patented and powerful Secure Connect Network (SCN). This architecture, designed exclusively for the correctional industry, offers an integrated, adaptable, highly-reliable framework to deliver mission-critical applications with secure access, anywhere, anytime.

Secure Connect Network (SCN)

SECURUS has the distinct advantage of being the incumbent provider and manufacturer of the current platform installed throughout the Alaska DOC as well as the manufacturer of the Secure Call Network proposed in our offer. As the manufacturer of both platforms, SECURUS can insure a smooth transition in maintaining and importing inmate profile information from the current platform into the SECURUS Secure Connect Network with little to no impact in inmate telephone calling privileges.

SECURUS has a significant amount of experience spanning two decades of installing inmate telephone systems in a Department of Corrections environment. During the installation of each institution, SECURUS will work closely with the Alaska DOC to convert all telephones to the new services in a secure and timely manor. Once all services at an Institution are cutover to Secure Connect Network, a technician will be required to enter each location in which an inmate telephone is installed to conduct a final test as well as re-affirm location of the station set.

While traditional inmate calling systems require a significant amount of physical space for hardware accommodation, the SECURUS Secure Call Network is able to service a facility (and in certain circumstances multiple facilities) from a single 4' Rack of equipment. For future expansions and additions to the inmate calling system, the simple addition of an additional Integrated Access Device (IAD) is most often all that is needed. The open architecture of Secure Connect Network is designed to accommodate the facility's needs rather than requiring the facility to adapt to the inmate calling system's functionality.

With the SECURUS Secure Connect Network, the chance of total system failure is essentially eliminated because in the event that any one component fails, the system will automatically switch to another, properly functioning component – in most cases with no disruption to service.

The SECURUS Secure Connect Network is a centralized processor located in a Class IV Disaster Resistant Carrier Class Data Center that is managed under the direct supervision and immediate hands-on maintenance of data center personnel.

The fail safes built in to the Secure Connect Network effectively prevent loss of data and system downtime because all of the data is stored in an offsite, centralized database and backed up at multiple locations. Because the system is web-based, the data can be accessed at any location with an internet connection, and SECURUS' Secure Connect Architecture maintains the system at the highest level of operability. SECURUS proactively identifies potential system and network abnormalities through our centralized suite of diagnostic applications called Sentinel. Sentinel continuously monitors your hardware, software, and system performance from our operations center in Dallas, Texas. This allows our dedicated personnel to diagnose and resolve issues on your system, often before you notice a problem yourself.

The infrastructure supporting the Secure Call Network was built from conception with high availability and full redundancy as part of the vision. 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

SECURE INSTANT MAIL HIGHLIGHTS:

- Eliminate Contraband
- Increased Investigative Abilities
- Increased Audit Capabilities
- Data stored and shared among multiple agencies
- Automated Key Word search with highlighting
- Automated and Patented transliteration from 12 foreign languages into English to avoid costly translations
- Integrated Mail Violation software for easy processing
- Automated funding of inmates' trust fund accounts to reduce staff labor
- Verify Mail Sender Information
- Secured and Encrypted Messaging to inhibit illegal activity
- Forward Internal Communication from Administration to inmates
- Additional Source of Revenue to the Department

automatic fail-over. As an example, our routers and servers have dual CPUs, NICs, power supplies, and A & B power feeds. The telecommunications circuits provided by our Telco Carriers feeding the network are both redundant and diverse.

SECURUS' centralized solution provides an advanced method of aggregating data and providing centralized management of a large system with many remote satellite sites. Each remote site is connected to a central site using MPLS (Multi Protocol Label Switching) T-1's for voice and data providing centralized management of user profiles. New or updated user profiles and system configuration data are archived at the central site for centralized management. Remote users have the ability to securely login to the centralized site when necessary to operate the system, change system configuration, troubleshoot, and retrieve data. The System security features at the central site strictly control this operation. System operators must have a security clearance based on passwords, user-IDs, and security levels to gain access to any individual features of the System. All changes to configuration are tracked based upon users' profiles and managed through levels of security access.

Secure Instant Mail™ (SIM)

SECURUS Secure Instant Mail™ (SIM) offers an independent, fully controlled, electronic mail communication between the inmates and their families and friends while providing correctional facilities with an array of investigative tools to inhibit inmates' illegal activities, and the influx of contraband into the Alaska DOC facilities helping to ensure public and Alaska DOC staff safety. Further, SIM retains sophisticated layers of security to protect the integrity of these correspondences as investigative tools.

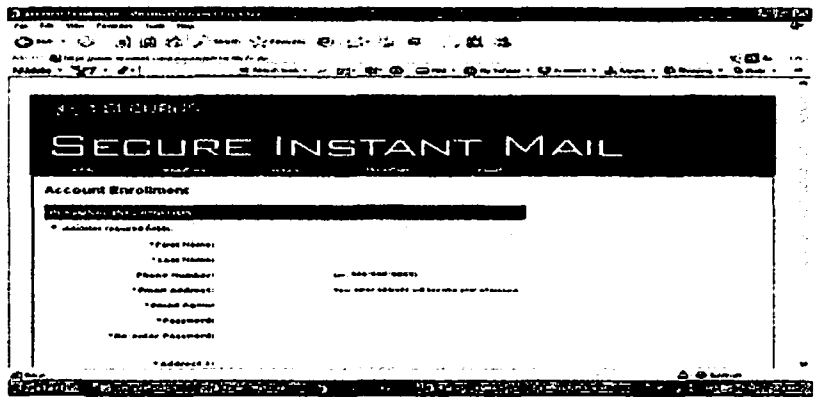
Secure Instant Mail is integrated with our Inmate Telephone System, thus providing the Alaska DOC's authorized personnel with the vast array of information readily available through the single entry point of Graphical User Interface (GUI).

Text only e-messages coming to authorized inmates within a correctional facility are created and sent by any individual from any personal computer after sender's identifying information is authenticated during an initial enrollment process. Facility personnel with proper authorization may access identifying information on the party sending the correspondence, which allows the Alaska DOC quality investigative information.

These correspondences are securely stored on the Secure Instant Mail server until they are downloaded, automatically sorted and printed upon review of the correctional staff on the dedicated terminal provided to each of the Alaska DOC correctional facility's mailroom. Inmates then receive a hard copy of approved correspondences, thus eliminating individual assessment of each individual correspondence for contraband.

With the Alaska DOC's approval, an inmate may write a return letter to the sender. Return letters are scanned into the system and automatically routed to originator. All incoming and outgoing e-messaging letters are digitally recorded, catalogued, stored and available to the Alaska DOC for investigative review at any time.

To further enhance correctional personnel investigative abilities, Secure Instant Mail™ automatically scans these correspondences and highlights any key words monitored by investigators through a customizable list of key words.



To reduce the Alaska DOC staff's manual labor hours and to increase operational efficiency, the Secure Instant Mail™ application provides inmates' families and friends with the option to electronically fund inmates' trust fund accounts. This feature is available at no additional cost, should the Alaska DOC elect to enable it.

All costs involved with Secure Instant Mail™ application will be borne by the inmates' families and friends that set up an account to use the feature. Rates are determined based on SECURUS' full commitment to provide affordable communication to the family and friends of inmates.

Secure Instant Mail is extremely user friendly and provides easy access to the Alaska DOC personnel to Secure Instant Mail investigative benefits.

Friends and Family Assistance

SECURUS has a comprehensive solution suite providing friends and family of incarcerated individuals complete assistance with account funding, account maintenance, and inquiries. Friends and family members are able to make payments through a wide variety of options: their local telephone companies, SECURUS direct billing, or through SECURUS' prepay payment methods. SECURUS also partners with a wide variety of national vendors to further facilitate transaction funding (i.e., Western Union, Ace Cash Express, etc...) and is open to partnering with other vendors as well. The goal of our comprehensive set of funding enablers is to facilitate communication. In order to facilitate communication and provide conveniences to friends and family members of inmates, it is necessary to maximize the types of payment methods (personal checks, credit cards, debit cards, money orders, etc.) and provide the most avenues to accept payments (Western Union, ACE Cash Express, website, etc.).

To provide alternatives to people who want to expedite the account funding process without the inconvenience or expense associated with sending the payment via overnight mail we propose to offer convenience payment alternatives such as credit cards, debit cards, Western Union, and ACE Cash Express that do require a payment convenience fee.

It is SECURUS' goal to reduce the burden on the Alaska DOC personnel by optimizing the convenience to the public and providing answers to any questions raised by friends and family members of inmates. Facilities can significantly reduce staff involvement allowing SECURUS to handle routine questions and issues that arise. The funding options suite provides a number of self-service and assisted channels for funding accounts and resolving friends and family issues related to communications. In addition, because our funding options enable more calls to connect, revenues to the state will increase, and costs to the state will decrease. Our diverse funding solutions have several sources of assistance. They are:

- 24X7 Automated Phone Access
- "Live Person" Call Center Access
- Web Site Access

Our suite of funding options ensures that friends and family have unlimited access to fund and maintain accounts in order to ensure their ability to receive inmate communications – without consuming limited facility staff resources. Everything in the funding enabler suite focuses on increasing an inmate's chance to successfully connect and maintain contact with friends and family.

Automated Phone Access

Automated Phone Access turns any phone into powerful account maintenance and funding tool, available 24 hours a day, 7 days a week. This touch-tone controlled application assists callers with easy access to account funding and informational aid from any standard telephone. Callers have the ability to dial directly into the system, where an automated assistant guides them through every step. Make payments (Personal Checks or Credit Cards)

Automated Phone Access is a standard part of the funding enabler suite at no charge to the Alaska DOC.

Call Center Access

SECURUS' call centers provide a staff of trained professionals, backed by a state-of-the-art automated call processing system, to assist friends and family with account information, maintenance, and funding questions. SECURUS' call centers are the only nationwide customer care centers dedicated solely to the correctional industry. SECURUS will provide a toll free number, 800-844-6591, specifically for friends and families of inmates. These calls will be directed to 350 SECURUS Customer Care Specialists capable of assisting the

Alaska DOC customers, and all of our representatives are specifically trained to handle account inquiries that arise in this very specialized industry. Customer Care Specialists provide callers with all of the information necessary in order to have complete control over all of their account activity. All of our call centers are benchmarked with monthly customer satisfaction ratings, which are measured by our customers (friends and family members accepting calls from inmates and the Alaska DOC).

Web Site Access

SECURUS' Customer Web Site specializes in assisting friends & family members who have access to the Internet. Accessible via the Correctional Billing Services Web Portal (https://www.correctionalbillingservices.com/), the online site provides access to vital customer information 24 hours a day, 7 days a week. Web Site users can also access all of their funding options as well as important facility information at the touch of a button.

The easy to use Call Center, Web Site interface, and Automated phone access ensures secure, intuitive, self-service access for handling all account needs, including:

- Confirm per minute rates on phone calls
- Obtain billing information
- Review call durations & history
- Fund prepaid phone accounts
- Provide Western Union payment information
- Receive notification of new service availability (ex: Secure Instant Mail, Voice Mail)
- Confirm originating facility
- Review account balances
- Turn on/off user account notifications

The extraordinary value of our suite of funding options results from the increase in communication between the inmate and their friends and family members. This occurs by increasing payment types and payment avenues, which eases the funding process of friends and family members of inmates. This value ultimately benefits the facility through decreased cost and increased revenue.

The entire funding options portfolio provides a comprehensive set of funding and account management channels that are unique in the industry. While other competitors may offer point solutions, no other competitor is able to offer the breadth of centralized integrated funding enablers provided by SECURUS via Automated Phone Access, Call Center Access, and Web Site

Access. Simply stated – there is no combined competitive offering comparable in the industry today.

Service Excellence

We understand that the best service is provided by a tech and service rep that has an intimate knowledge of each facility. To maintain the highest levels of service availability and personal touch, Alaska DOC facilities will benefit from our incumbent position. Not only is your SECURUS account team intimately familiar with the inter workings of the individual facilities but all of our service personnel are factory certified and trained in the maintenance of our systems resulting in unmatched support and service.

SECURUS proactively identifies potential system and network abnormalities through our centralized Network Operations Centers (NOC). Each center continuously monitors your hardware, software, and system performance to assure our client's with a 99.9% operational uptime. This allows our dedicated personnel to diagnose and resolve issues on your system, before you notice a problem yourself. Our experience has shown a reduction of direct facility service issues by approximately 40% for facilities that utilize vendors without pro-active NOC monitoring. Most importantly, our systems are engineered and implemented to provide the highest levels of redundancy to maximize system-wide availability and minimize downtime. A more detailed analysis is contained herein.

Offer Summary

We have crafted a balanced financial package that offers an aggressive return to the Alaska DOC with attractive local and long distance collect call rates to the inmates and their families.

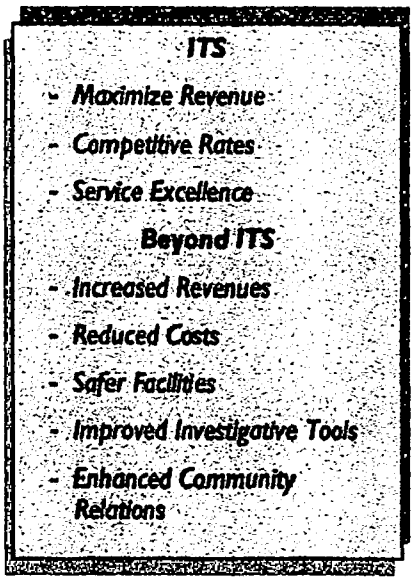
SECURUS is proposing to use GCI as a partner to provide local collect calling services. GCI will be obtaining required regulatory approvals from the Regulatory Commission of Alaska for a local collect calling rate.

As we have patented technology that results in more connected calls, we believe the goal to maximize the Alaska DOC revenues will be met. Inmates and their families will also be pleased with competitive rates, innovative new communication opportunities and gold standard service.

We believe our proposal surpasses established requirements of the ITS. We also believe our revolutionary revenue generating programs will exceed your revenue requirements while offering friends and family a suite of funding enablers. We are committed to completing more calls, creating new connection opportunities, introducing innovative methods of communication, and enhancing security and investigative capabilities. SECURUS will demonstrate its commitment to operational excellence by performing systematic upgrades to the Inmate Telephone System throughout the term of this Agreement.

While other proposals will be principally based upon a commission percentage and call rate, it is clear the SECURUS offering goes much further. We believe our very competitive commission offer, our ability to maximize inmate calling revenue and our technology-driven operating efficiencies will produce a superior economic return to the Alaska DOC that far beyond commission alone.

SECURUS is the largest, most experienced, and we believe the best Inmate Telephone Service enterprise in the industry. We also believe our value to the State goes well beyond the ITS foundation. It is in our approach and in the combination of delivered ITS value and beyond that expose the full potential of an Alaska DOC and SECURUS Technologies Partnership that will be realized and felt throughout our relationship.



We thank you for your time and consideration, and we respectfully request the opportunity to serve the Alaska DOC.

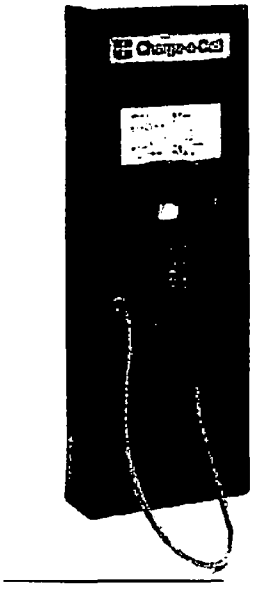
Month	Gross Revenue	Commission Percentage	Commission Earnings
13	$240,000.00	23%	$55,200.00
14	$245,000.00	23%	$56,350.00
15	$250,000.00	23%	$57,500.00
16	$250,000.00	23%	$57,500.00
17	$250,000.00	23%	$57,500.00
18	$250,000.00	23%	$57,500.00
19	$275,000.00	23%	$63,250.00
20	$280,000.00	23%	$64,400.00
21	$290,000.00	23%	$66,700.00
22	$300,000.00	23%	$69,000.00
23	$300,000.00	23%	$69,000.00
24	$325,000.00	23%	$74,750.00
Year Two	$3,255,000.00	23%	$748,650.00
Actual Annual Revenue Commission Rate Attainment is 29%			
Revenue	$3,255,000.00	29.0%	$943,950.00
Earned			$748,650.00
Advance Payment			$100,000.00
Year Two True Up Payment			$95,300.00
Run Rate Commission for next 12 months			
Based on previous year revenue of $3,255,000 new monthly commission is 29.0%			

Attachment C

Equipment Specifications

Telephone Equipment Specifications

ITC7042BL Full Size Blue Inmate Phone with Volume Control



THE INDUSTRY STANDARD

- The overwhelming choice for State Prison Systems, The Federal Bureau of Prisons and County Facilities nationwide.
- Proven reliability, durability, and flexibility.
- DuraClear® Technology is Here!

APPLICATIONS:

- Prisons, inmate facilities
- Airports, courtesy phones, taxi phones
- Universities, schools
- Any location where coinless is a low maintenance, low cost alternative

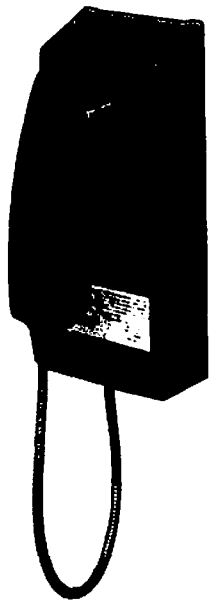
ORDERING OPTIONS:
ITC7042BL Full Size Blue Phone with VC
ITC7042BL/DC Full Size Blue Phone with DuraClear® and Volume Control

Wintel® **A Division of Independent Technologies**

FEATURES:

- 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.
- Built-in user controlled volume "LOUD" button for ADA mandated volume control (must be user-controlled volume amplification AND volume must reset to normal with on-hook to meet ADA requirements)
- Powder Coated cold rolled steel provides rugged vandal resistant telephone housing designed and built for inmate use
- Confidencer technology, built into every dial, filters out background noise at the user's location, allowing better sound to the called party
- Heavy chrome metal keypad bezel, buttons, and hookswitch lever withstand abuse and vandalism
- Armored handset cord is equipped with a steel lanyard (1000# 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 (DF4USA-75652-CC-E)

ITC7010 Mini Coinless Phone with Volume Control



THE INDUSTRY STANDARD:

- The overwhelming choice for State Prison Systems, The Federal Bureau of Prisons and County Jails nationwide.
- Proven reliability, durability, and flexibility.
- DuraClear® Technology Is Here!

APPLICATIONS:

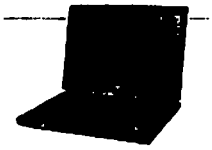
- Prisons, inmate facilities
- Airports, courtesy phones, taxi phones
- Universities, schools
- Any location where coinless is a low maintenance, low cost alternative

ORDERING OPTIONS:
ITC7010BL Mini Blue Phone with Volume Control
ITC7010SS Mini Phone in Stainless Steel, with VC
ITC5010BL Mini Blue Phone

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). *ITC7 series features Volume Control.*
- Brushed stainless steel and powder coated cold rolled steel provide rugged vandal resistant telephone housing designed for inmate 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 hookswitch lever withstand abuse and vandalism
- Armored handset cord is equipped with a steel lanyard (1000# 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 (DF4USA-75652-CC-E)

Dell Latitude D620 ATG (Intel Core 2 Duo T5500



Full specifications for Dell Latitude D620 ATG (Intel Core 2 Duo T5500 1.66GHz 2M L2 Cache, 667Mhz Dual Core, 80GB HDD, 512MB RAM)

Manufacturer: Dell, Inc.
Part number: BLCWH1S

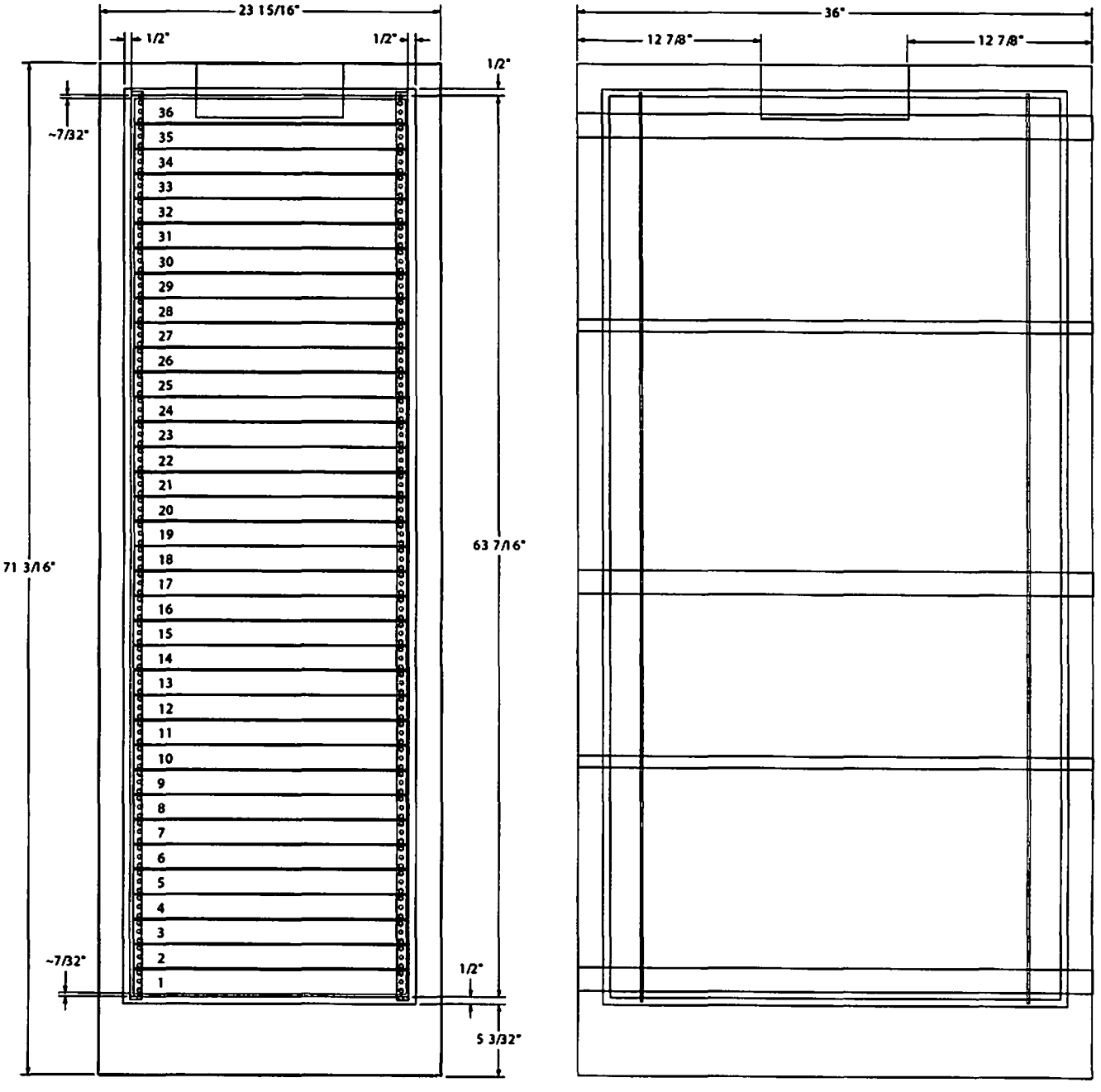
GENERAL	
System Type	Notebook
Built-in Devices	Speaker, Wireless LAN antenna
Rugged Design	Yes
Width	13.5 in
Depth	9.4 in
Height	1.7 in
Weight	6.2 lbs
Notebook type	Mid-size laptops (6-7.5 lbs.)
Screen type	Wide-screen
Wireless Capabilities	802.11g, 802.11b
PROCESSOR	
Processor	Intel Core 2 Duo T5500 / 1.66 GHz
Multi-Core processor technology	Dual-Core
64-bit processor	Yes
Data bus speed	667 MHz
Chipset type	Mobile Intel 945GM Express
CACHE MEMORY	
Type	L2 cache
Cache size	2 MB
RAM	
Installed Size	512 MB / 4 GB (max)
Technology	DDR II SDRAM - 667 MHz
RAM configuration features	1 x 512 MB
STORAGE CONTROLLER	
Storage controller type	Serial ATA/IDE
STORAGE	
Floppy Drive	None
Hard Drive	80 GB - Serial ATA-150 - 7200
Storage Removable	None
Hard drive type	Portable
OPTICAL STORAGE	
Type	CD-RW/DVD
CD / DVD read speed	24X

TELECOM	
Modem	Fax / modem
Max transfer rate	56 Kbps
Protocols & Specifications	ITU V.92
NETWORKING	
Networking	Network adapter
Networking / Wireless LAN Supported	Yes
Wireless NIC	Dell Wireless 1390
Data link protocol	Ethernet, IEEE 802.11b, IEEE 802.11g, Fast Ethernet, Gigabit Ethernet
Networking standards	IEEE 802.11b, IEEE 802.11g
EXPANSION / CONNECTIVITY	
Expansion Slots Total (Free)	2 (1) x Memory, 1 (1) x PC Card - Type I/II, 1 (1) x Smart Card
Interfaces	1 x Display / video - VGA - 15 pin HD D-Sub (HD-15), 1 x Serial - RS-232 - 9 pin D-Sub (DB-9), 1 x Microphone - Input, 1 x Audio - Line-out/headphones - Mini-phone stereo 3.5 mm, 4 x Hi-Speed USB - 4 pin USB Type A, 1 x Network - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45, 1 x Modem - Phone line - RJ-11, 1 x Docking / port replicator, 1 x Infrared - IrDA
MISCELLANEOUS	
Compliant Standards	EPEAT Silver, MIL-STD 810F
POWER	
Power device form factor	External
Voltage Required	AC 120/230 V
BATTERY	
Technology	6-cell Lithium Ion
Installed Qty	1 / 2 (max)
Battery capacity	56 Wh
OPERATING SYSTEM / SOFTWARE	
OS Provided	Microsoft Windows XP Home Edition, SP2, with media
Software type	Cyberlink PowerDVD, Drivers & Utilities
MANUFACTURER WARRANTY	
Service & support type	3 years warranty
Service & Support Details	Limited warranty - 3 years
ENVIRONMENTAL PARAMETERS	
Min operating temperature	32 °F
Max operating temperature	95 °F
Operating humidity range	10 - 90%
Shock Tolerance	142 g @ 2ms half-sine pulse (operating) / 163 g @ 2ms half-sine pulse (non-operating)
Vibration Tolerance	1.04 g @ RMS (random) (operating) / 7.69 g @ RMS (random) (non-operating)
CNET LABS' BENCHMARKS	
CNET Labs battery drain test: DVD Playback (min)	235

Attachment D

Manufacturer's Cut Sheets (Racks)

REVISIONS				
ZONE	LTR	DESCRIPTION	DATE	APPROVED



SITE NAME: _____

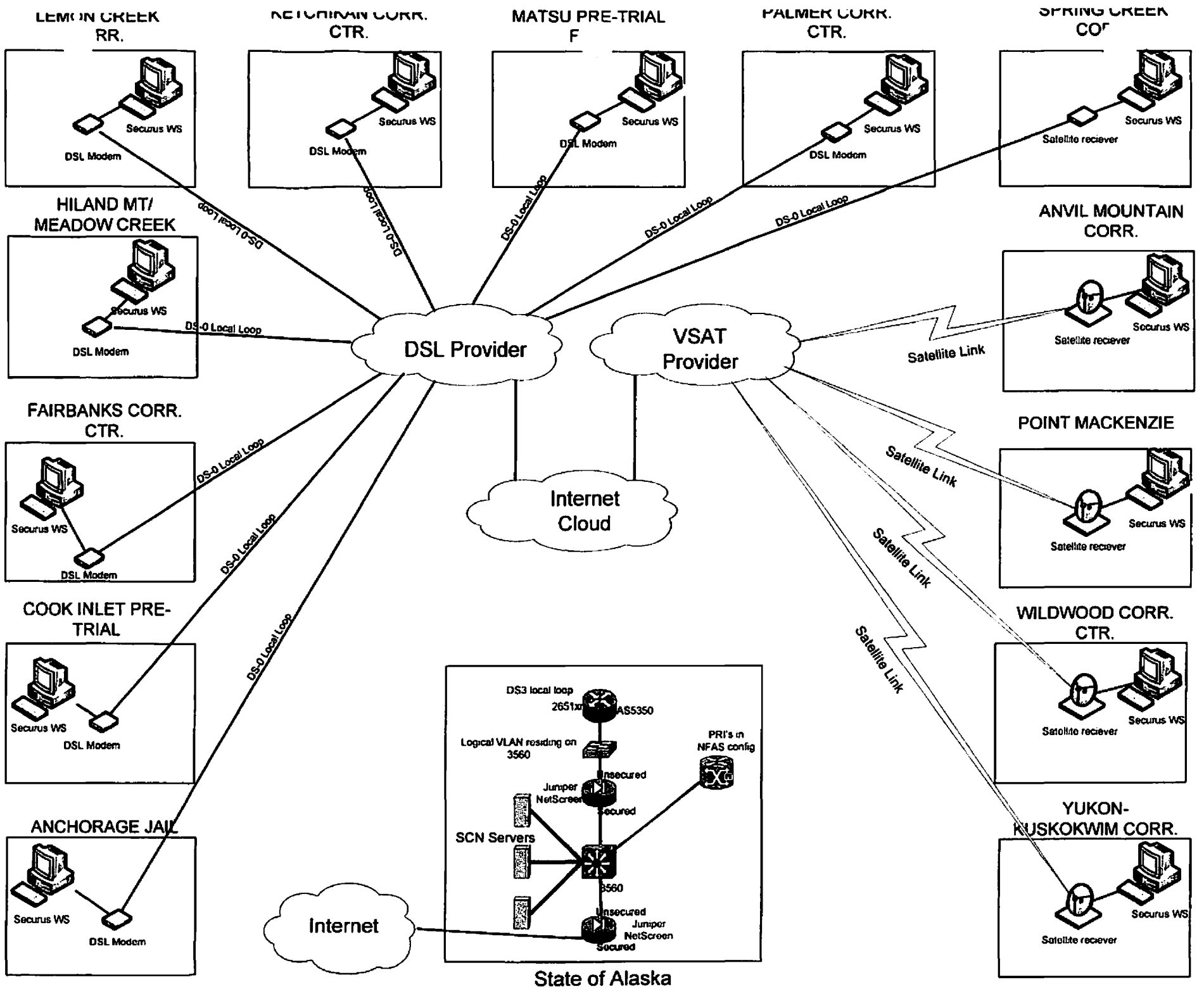
SITE LOCATION: _____

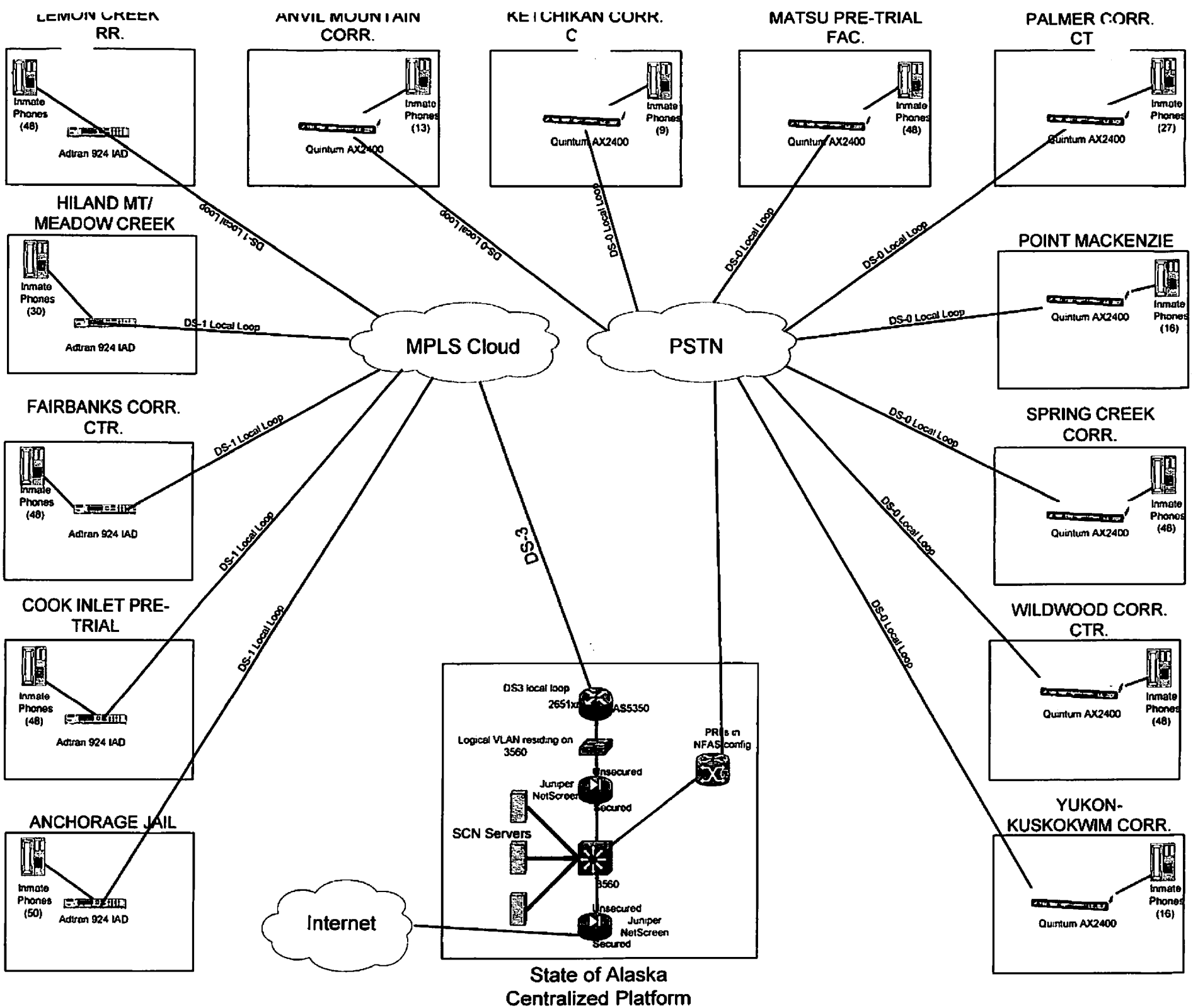
_____

RACK # ____ of ____

TOLERANCES	MATERIAL	T-NETIX INC.
X ± 0.010"	FINISH	67 INVERNESS DRIVE EAST ENGLEWOOD, COLORADO U.S.A. 80112
XX ± 0.005"	APPROVALS / DATE	TITLE: 36U B-Line -Evercom Cabinet
ANGLES ± 0.5 Deg	DRAWN BY: S.D. PASSE 1/20/00	SIZE: D
HOLES ± 0.003"	CHECKED BY	CODE
SCALE: 1/2		NUMBER
		REV.
		DATE 1/20/00 SHEET 1 OF 1 PAGE 1 OF 1

Attachment E
Line Diagrams

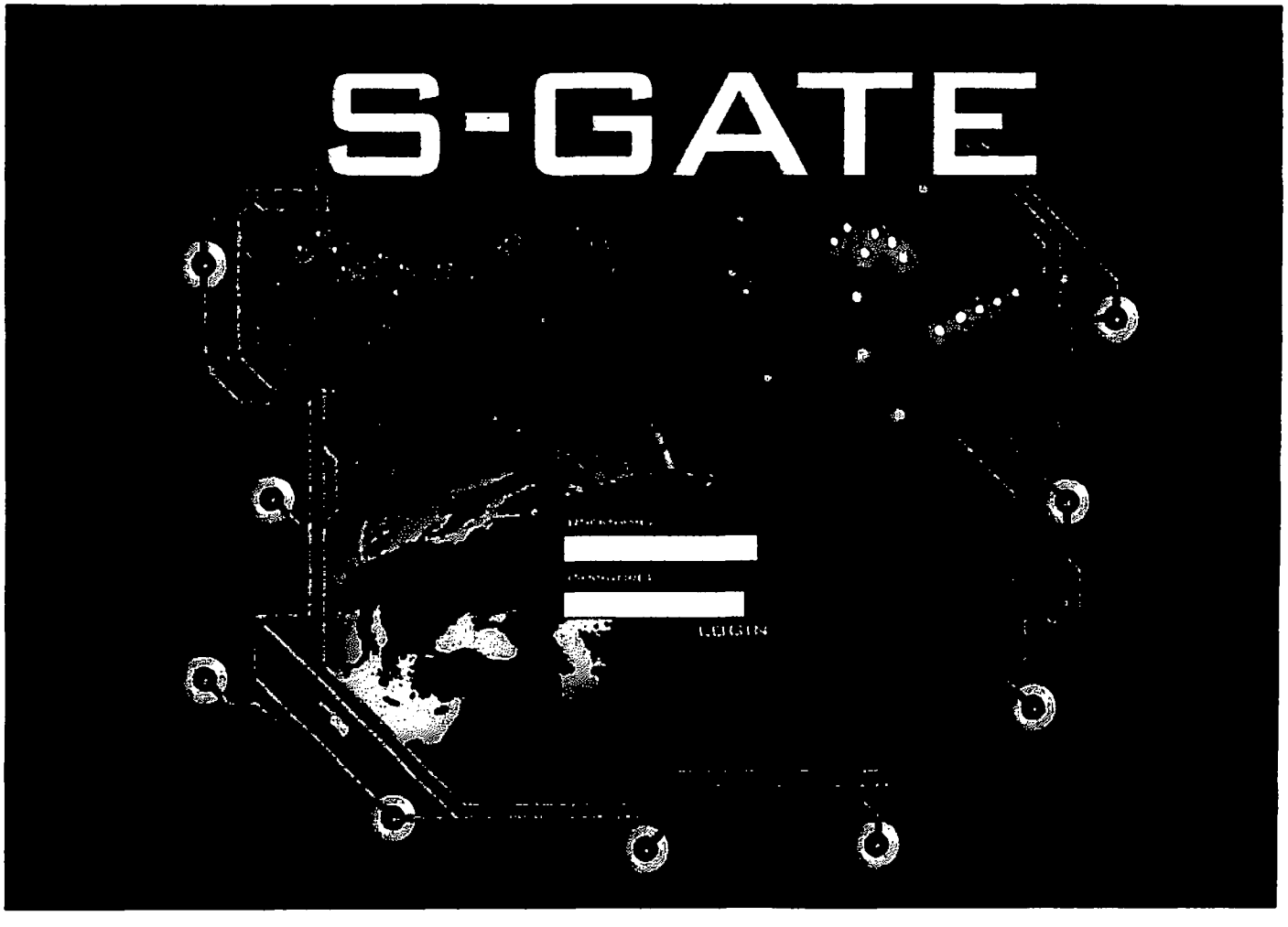

LEMON CREEK RR.
KETCHIKAN CORR. CTR.
MATSU PRE-TRIAL F
PALMER CORR. CTR.
SPRING CREEK COR
Securus WS
DSL Modem
Satellite reciever
HILAND MT/ MEADOW CREEK
ANVIL MOUNTAIN CORR.
DS-0 Local Loop
DSL Provider
VSAT Provider
Satellite Link
FAIRBANKS CORR. CTR.
POINT MACKENZIE
Internet Cloud
COOK INLET PRE-TRIAL
WILDWOOD CORR. CTR.
ANCHORAGE JAIL
YUKON-KUSKOKWIM CORR.
DS3 local loop
2651xm
AS5350
Logical VLAN residing on 3560
PRI's in NFAS config
Unsecured
Juniper NetScreen
Secured
SCN Servers
3560
Internet
State of Alaska
Centralized Platform


LEMON CREEK RR.
Inmate Phones (48)
Adtran 924 IAD
ANVIL MOUNTAIN CORR.
Inmate Phones (13)
Quintum AX2400
KETCHIKAN CORR. C
Inmate Phones (9)
Quintum AX2400
MATSU PRE-TRIAL FAC.
Inmate Phones (48)
Quintum AX2400
PALMER CORR. CT
Inmate Phones (27)
Quintum AX2400
HILAND MT/ MEADOW CREEK
Inmate Phones (30)
Adtran 924 IAD
DS-1 Local Loop
DS-0 Local Loop
POINT MACKENZIE
Quintum AX2400
Inmate Phones (16)
MPLS Cloud
PSTN
FAIRBANKS CORR. CTR.
Inmate Phones (48)
Adtran 924 IAD
SPRING CREEK CORR.
Quintum AX2400
Inmate Phones (48)
COOK INLET PRE-TRIAL
Inmate Phones (48)
Adtran 924 IAD
DS-3
WILDWOOD CORR. CTR.
Quintum AX2400
Inmate Phones (48)
ANCHORAGE JAIL
Inmate Phones (50)
Adtran 924 IAD
DS3 local loop
2651xm
AS5350
Logical VLAN residing on 3560
PRIs on NFAS config
Unsecured
Juniper NetScreen
Secured
SCN Servers
3560
Unsecured
Juniper NetScreen
Secured
YUKON-KUSKOKWIM CORR.
Quintum AX2400
Inmate Phones (16)
Internet
State of Alaska
Centralized Platform

Attachment F

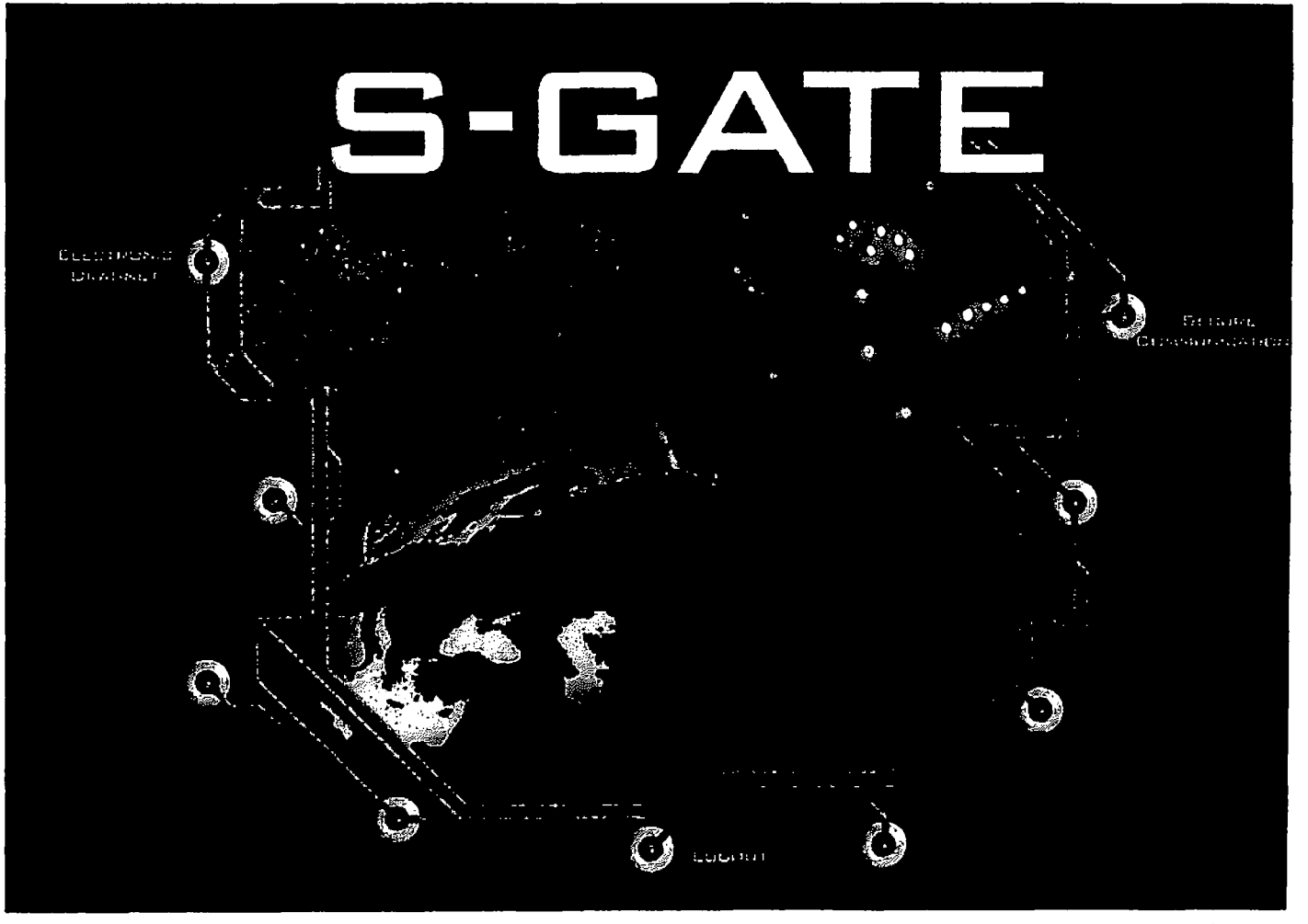
SECURUS User Interface Screens

SCP S-GATE Portal User Login



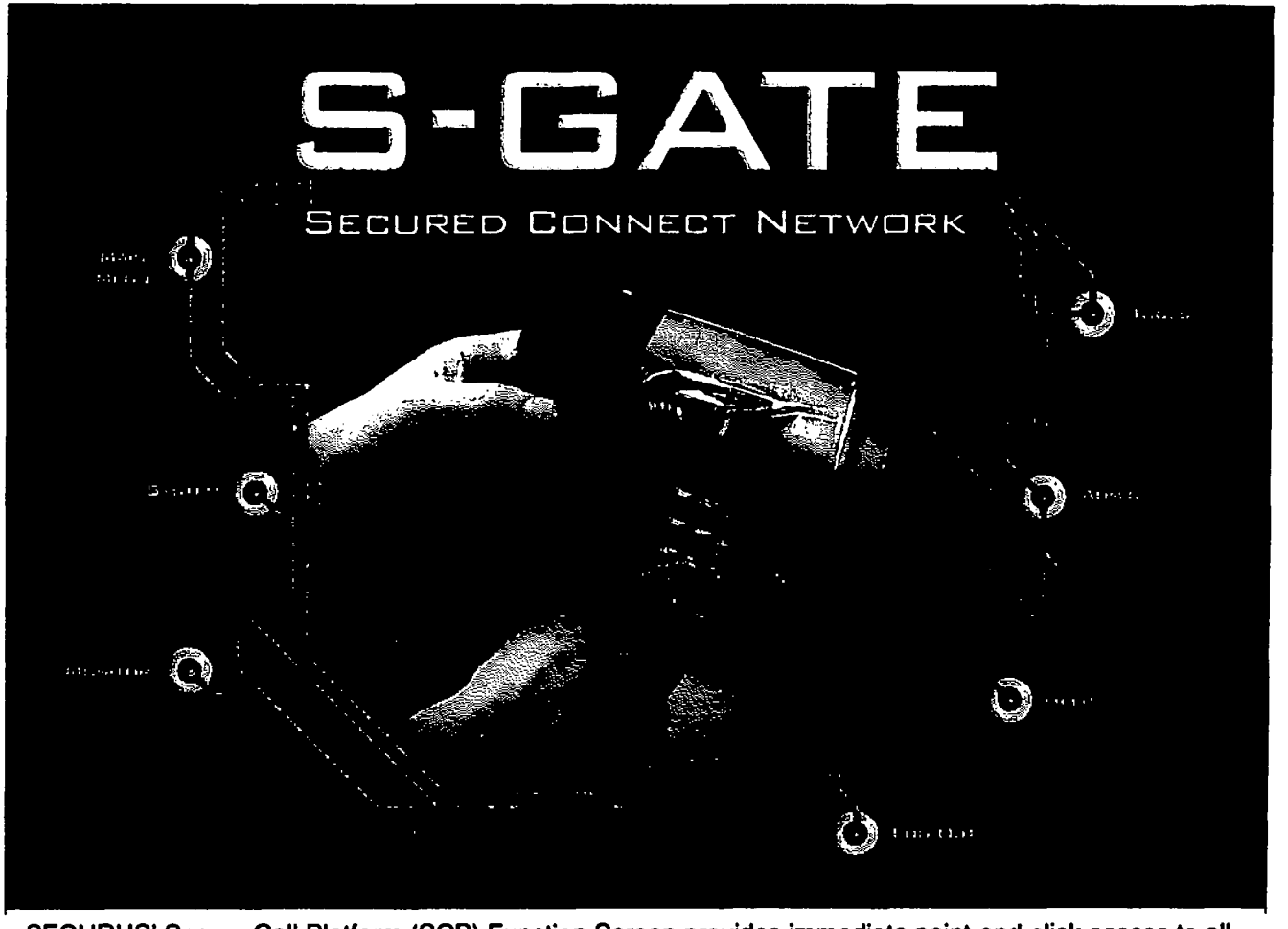
SECURUS' Secure Call Platform (SCP) login screen provides all authorized users secured access through the S-GATE portal to all contracted applications.

SCP S-GATE Portal Main Page



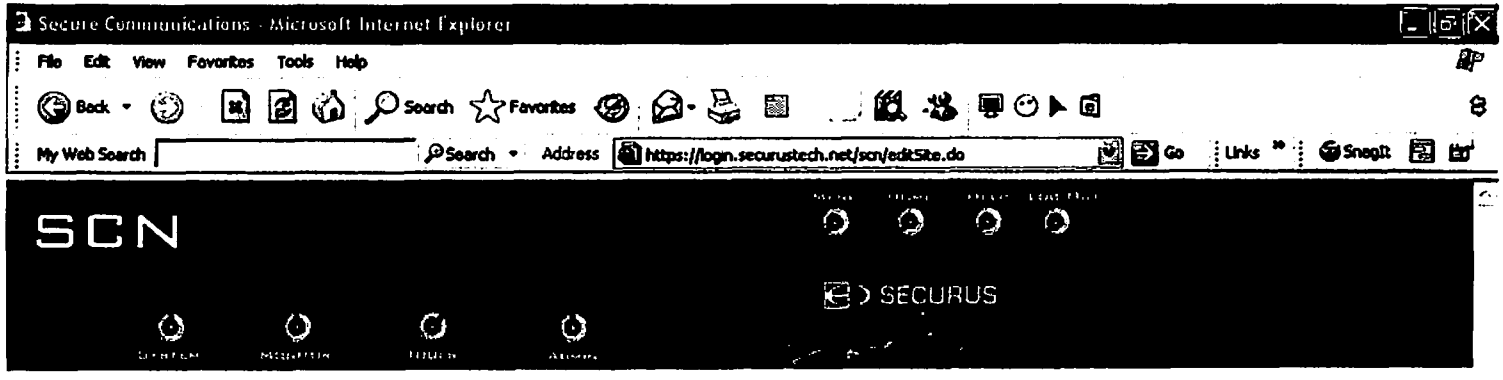
SECURUS' Secure Call Platform (SCP) S-GATE Portal Main page displays all customer contracted applications.

SCP Functions Screen



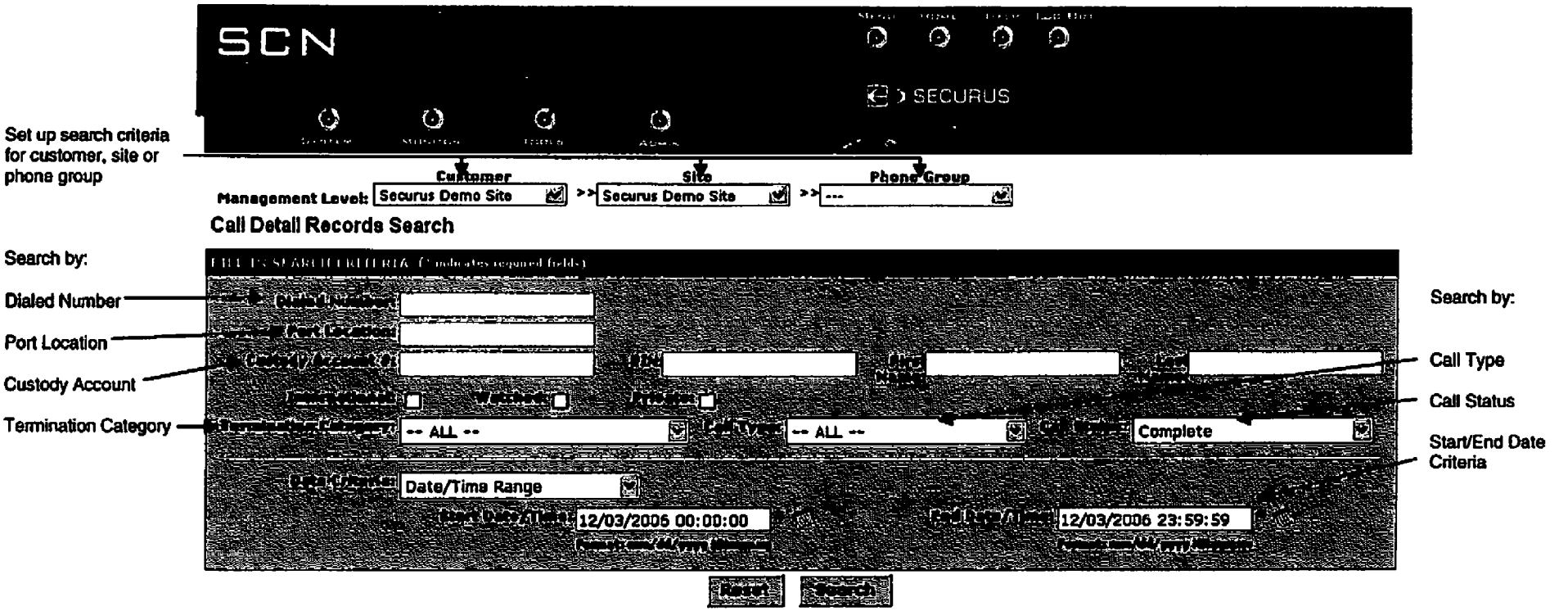
SECURUS' Secure Call Platform (SCP) Function Screen provides immediate point-and-click access to all application functions and modules.

SCP User Interface (UI) Navigation Bar



SECURUS' Secure Call Platform User Interface Navigation Bar is accessible from any page within the application and provides users easy access to all menu options, features, functions and modules.

Call Detail Search Criteria Screen



Call Detail Records Search criteria page is used to set up search criteria for a selected date and time or date/time range to retrieve site specific information as it pertains to a selected dialed number.

Live Call Monitor

View and listen to calls in progress By:

Customer

Site

Phone Group

Terminate calls in progress

View phones/location from which calls are made

View and track persons making calls

View and track numbers being called

Select calls for remote conferencing and monitoring

View call history details for selected phone numbers or cell locations

Management Level: Customer: Securus Demo Site >> Site: Securus Demo Site >> Phone Group: ---

Play	Location	Acct No.	Dialed Number	City, St Fwd Seconds Priv Watch	Status
	MainHallFrnt /25	190905	6065871542	39	Dialing Called Party
	PineBluff-In /7	190848		248	Collecting Dial-To-Number
	MB In-2 /39	204093		22	Collecting Dial-To-Number
	MSU /18	152787	8592802196	848	Call in Progress
	P Bluff-in /25	154523	3367660882	768	Call in Progress
	MB In-3 /40	201133	6069209552	270	Call in Progress
	MSU /32	193646	2708261940	774	Call in Progress (3way Call Detected)
	MB In-1 /38	204386	2702424562	202	Call in Progress
	RDGVW B Left/16	177489	5702781817	926	Call in Progress
	P Bluff-in /24	200289	8594721629	275	Call in Progress
	LWC /29	196038	5027428508	880	Call in Progress
	MB In-4 /41	203275	8593634027	64	Dialing Called Party

Active Calls Only

Dialed Number	Call Date/Time
No Number	11-03-2006 08:04:15
No Number	11-03-2006 08:04:27
No Number	11-03-2006 08:39:40
8594913390	11-03-2006 09:10:21
6063378357	11-03-2006 09:55:26
6065420551	11-03-2006 09:55:57
No Number	11-03-2006 09:57:54
6063378357	11-03-2006 09:59:17
6062486760	11-03-2006 10:02:23
6057878277	11-03-2006 10:07:59
8598796396	11-03-2006 10:56:16
5028339047	11-03-2006 10:57:34
No Number	11-03-2006 10:58:56
2708261940	11-03-2006 11:10:27

Showing calls from MSU /18

Monitoring page is used to view and monitor live calls. It has additional features that allows users to terminate calls, forward calls for remote monitoring, view the historyof calls from selected locations, and view the history of calls placed to selected numbers.

Security Template

Management Level: Customer — Securus Demo Site

Create New Template

Create new security access templates

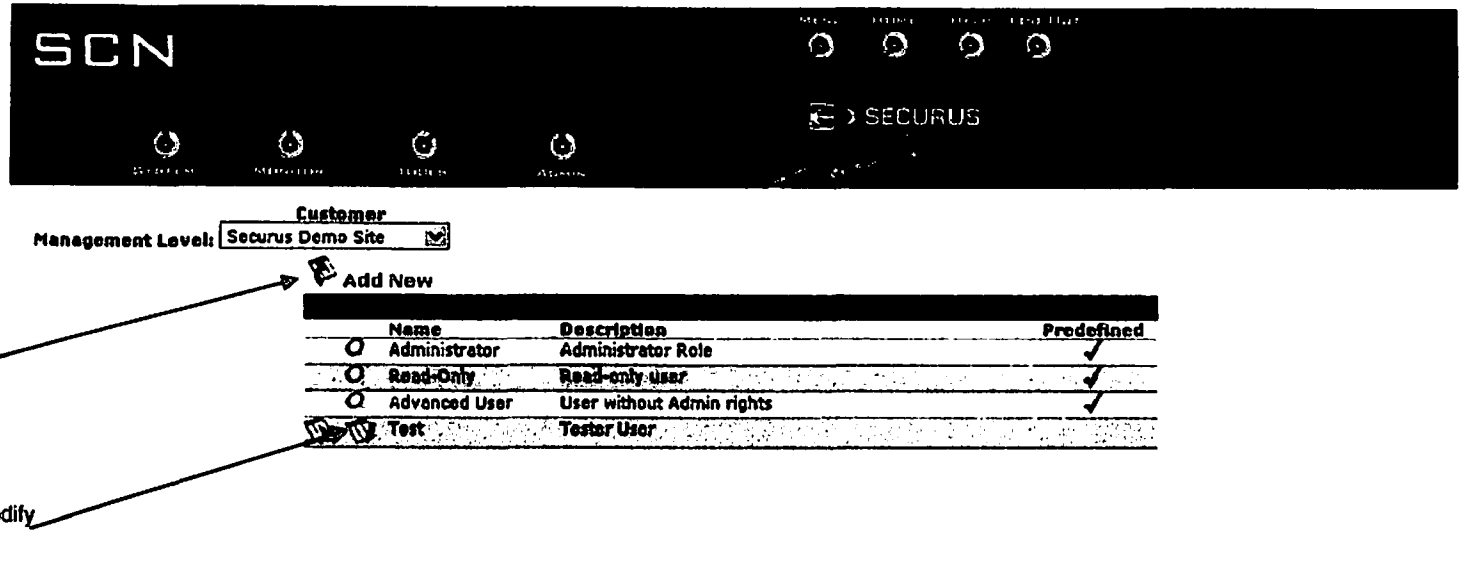
Select level of access for each module

Admin - Security Templates	☐	☐
Admin - User Management	☐	☐
Monitor - Forward Call	☐	☐
Monitor - Listen to Live Calls and Recordings	☐	☐
Monitor - Terminate Call Monitor	☐	☐
Monitor - Terminate Monitored Calls	☐	☐
Monitor - View Live Calls	☐	☐
Report - Call Detail	☐	
Report - Call Frequency	☐	
Report - Hourly Usage	☐	
System - Call Forward List Administration	☐	☐
System - Call Party Accounts	☐	☐
System - Call Schedules	☐	☐
System - Global Lists	☐	☐
System - Phone Group Config	☐	☐
System - Site Config	☐	☐

Cancel Create

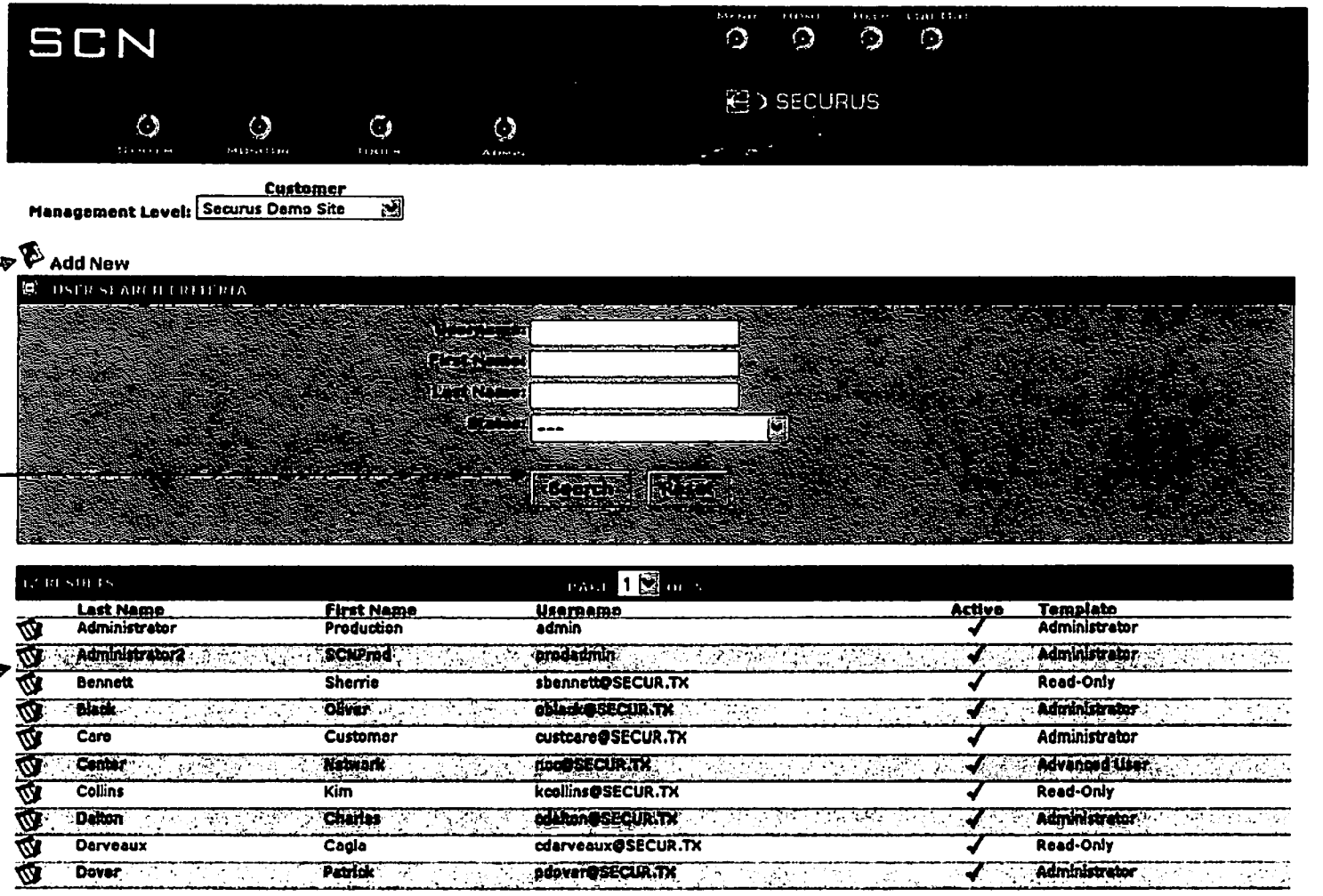
Security Templates page is used by site administrators to quickly create/design new templates to accommodate define access rights for specific roles on an as needed basis.

Role Editor



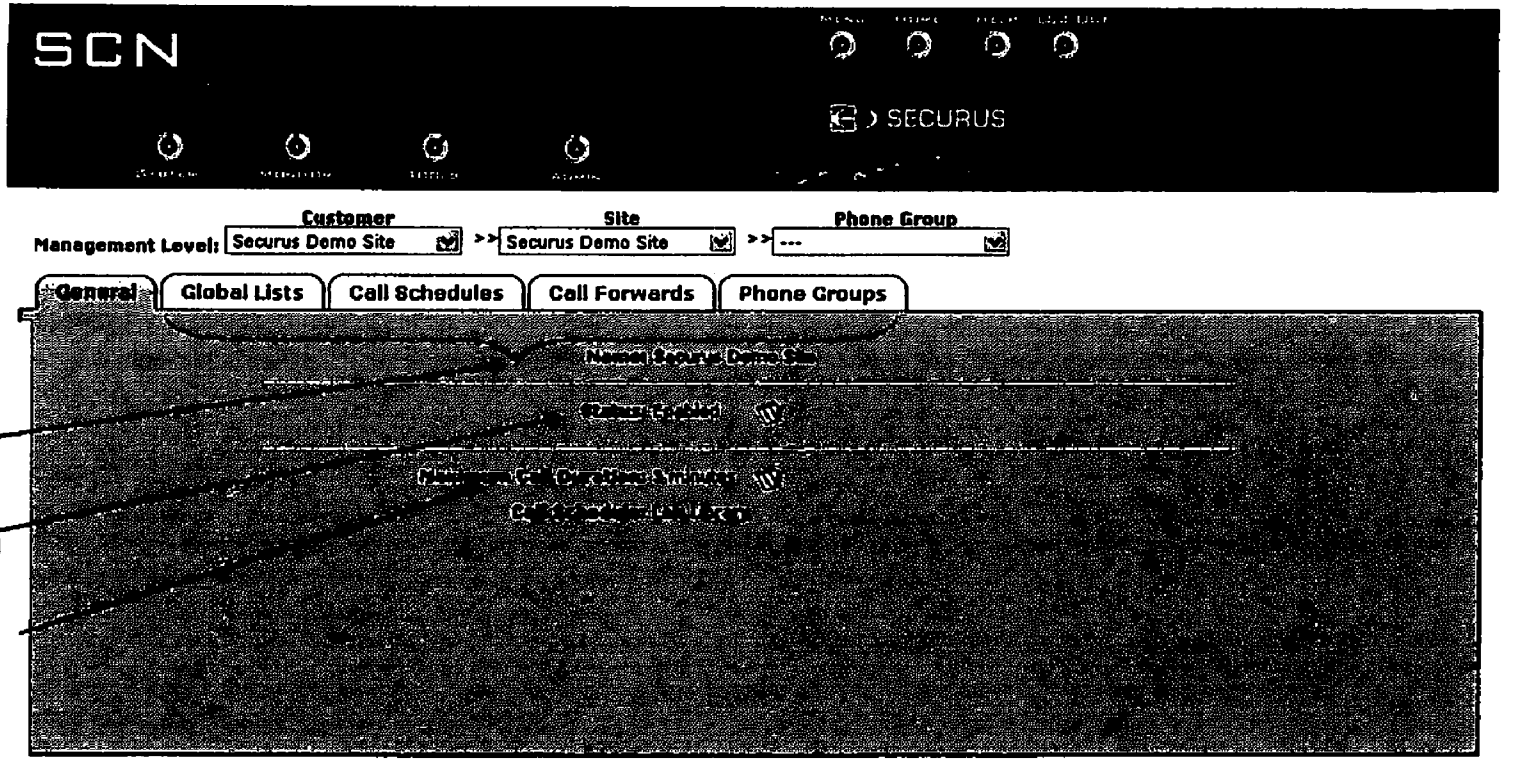
Role Editor Page is used by site administrators or users with administrative privileges to add new roles, edit, modify, and change or delete the privileges given to a specific role.

User Editor



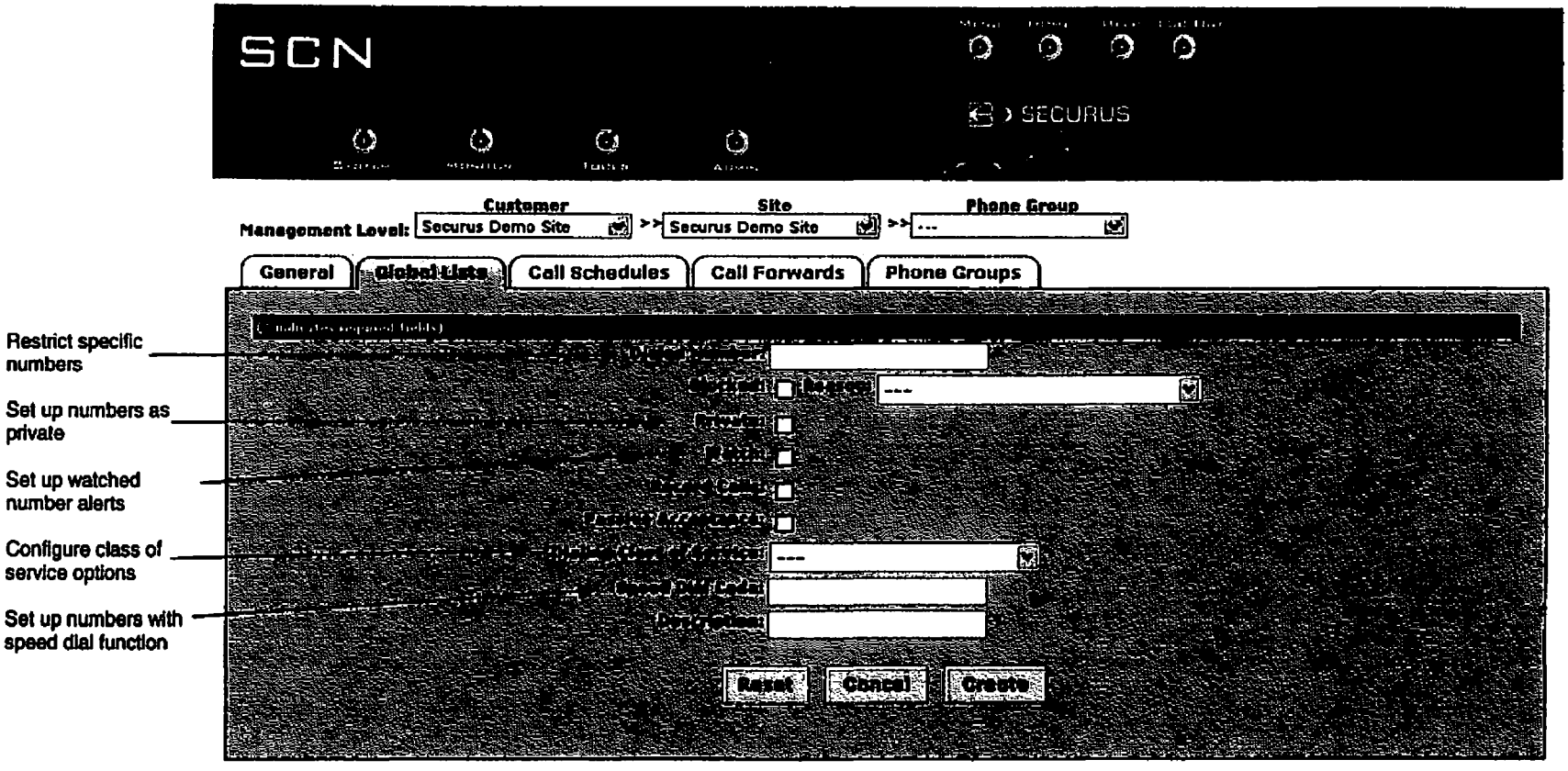
User Editor Page is used by site administrators or users with administrative privileges to update a current user's privileges

Site Modify & Setup Screen



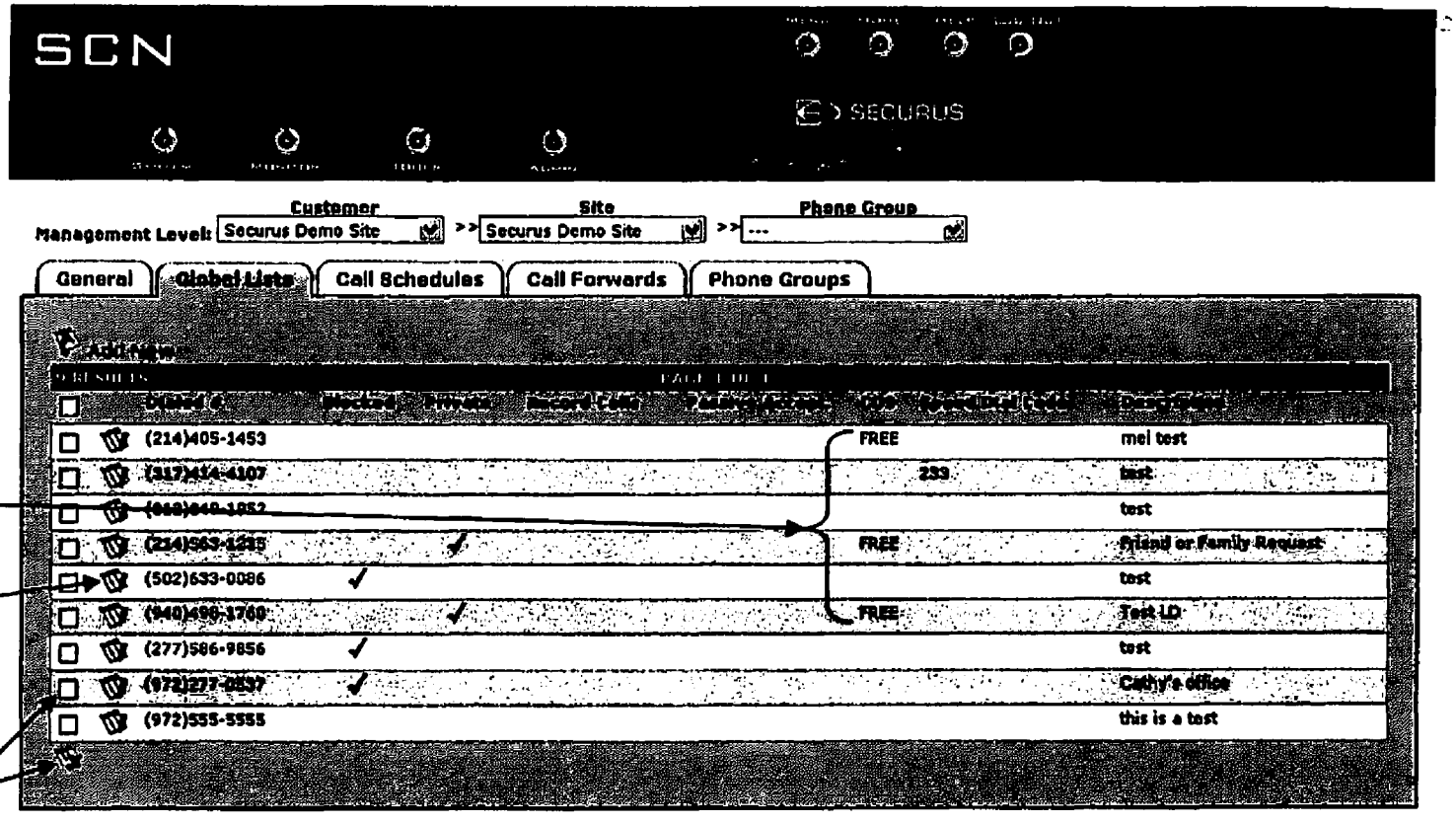
Site Modification Page is used display information about a site such as site name, phone groups, maximum allowable call duration, and the call schedule assigned to the site. Tabs provide users easy access to global list functions, call forwards, and phone group settings.

Global Lists Setup Screen



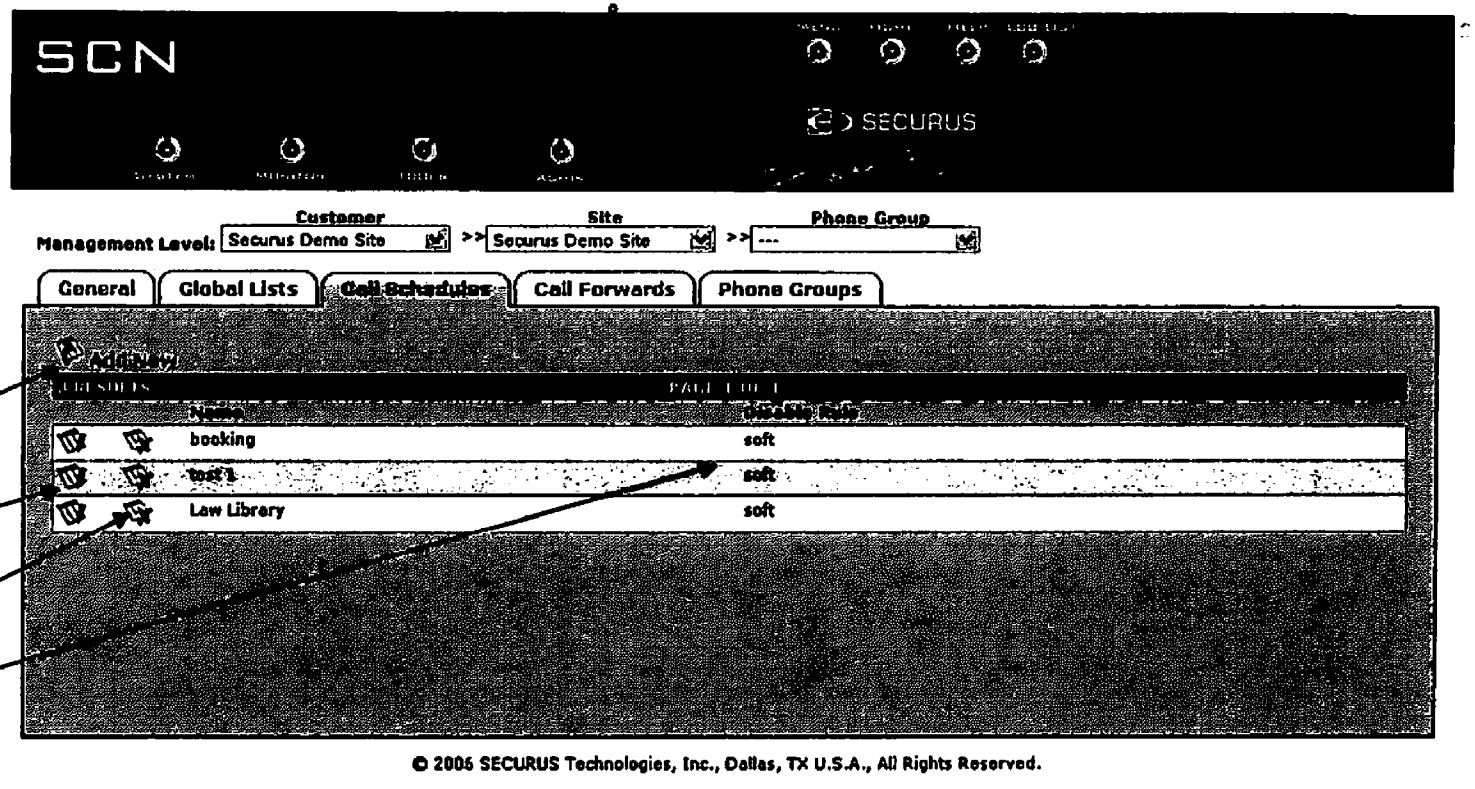
Global Lists Setup Page is used to configure dialing access and restrictions to called numbers. On this page users may configure and setup watched alerts, whether or not a called number is blocked or private, and also gives users the ability to define class of service and enter a speed dial code for the number.

Global Lists Editor Screen



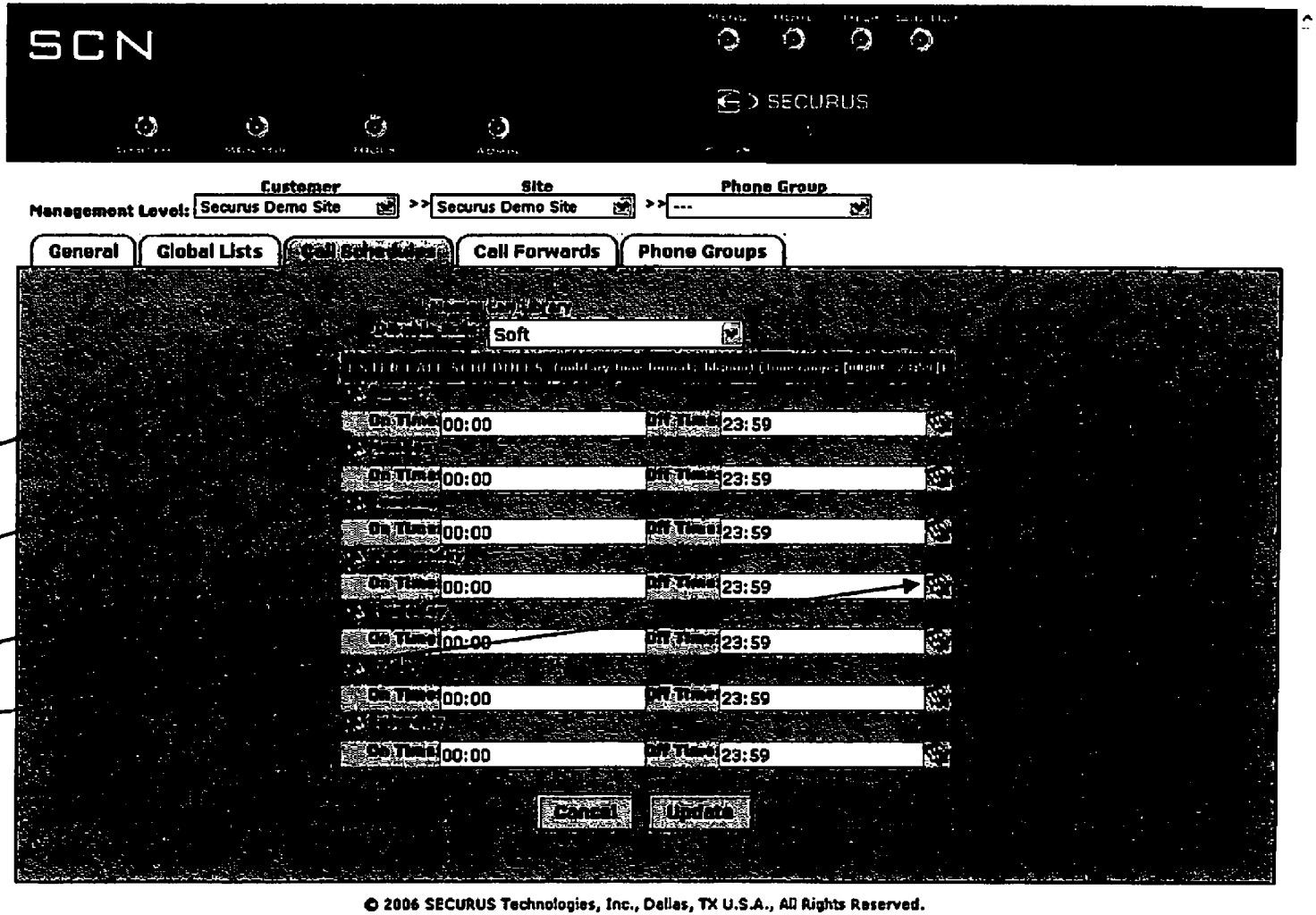
Global Lists Editor Page is used to view the status of a given number. Additionally authorized users are able to edit and change the status of numbers or remove old numbers from the lists.

Call Schedules Setup Screen



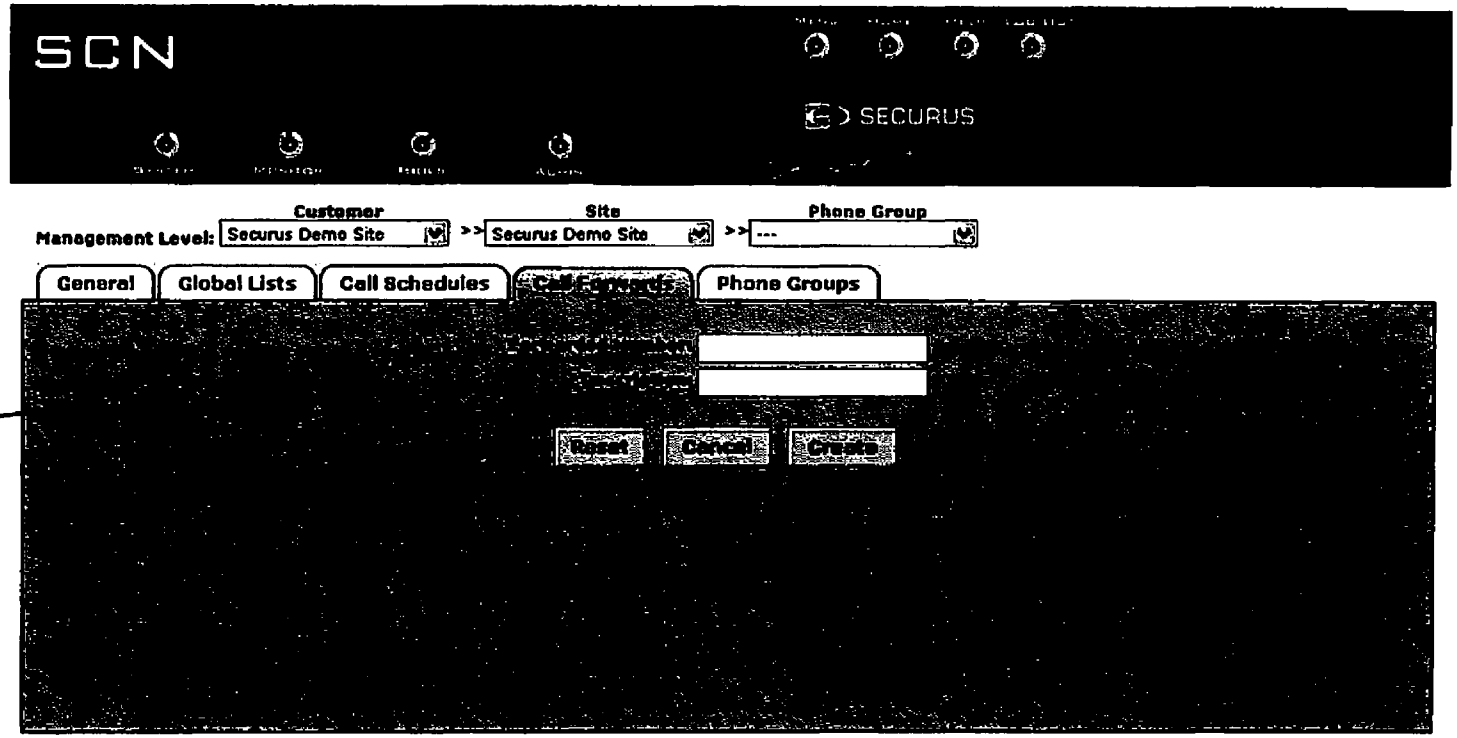
Call Schedules Setup Page is used to configure to allow customized phone use throughout the facility. Additionally, authorized users may edit call schedules to modify and make changer or delete a specific call schedule.

Call Schedules Editor



Call Schedules Editor Page is used to edit and make changes to system on/off call schedules or to assign multiple on/off times to a specific day on a selected call schedule. Additionally authorized users may configure enable/disable rules for each call schedule.

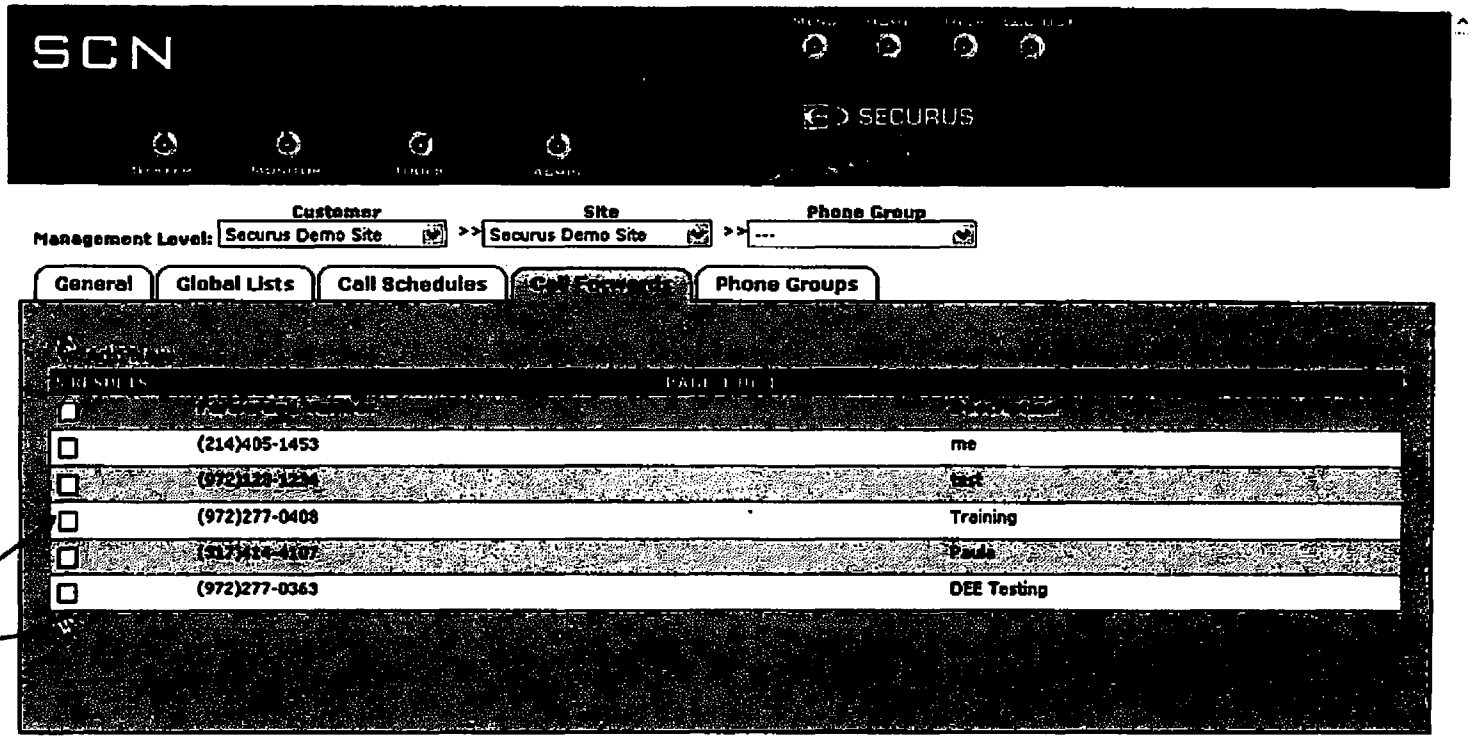
Call Forwards Setup Screen



Set up specific numbers to which live calls may be forwarded

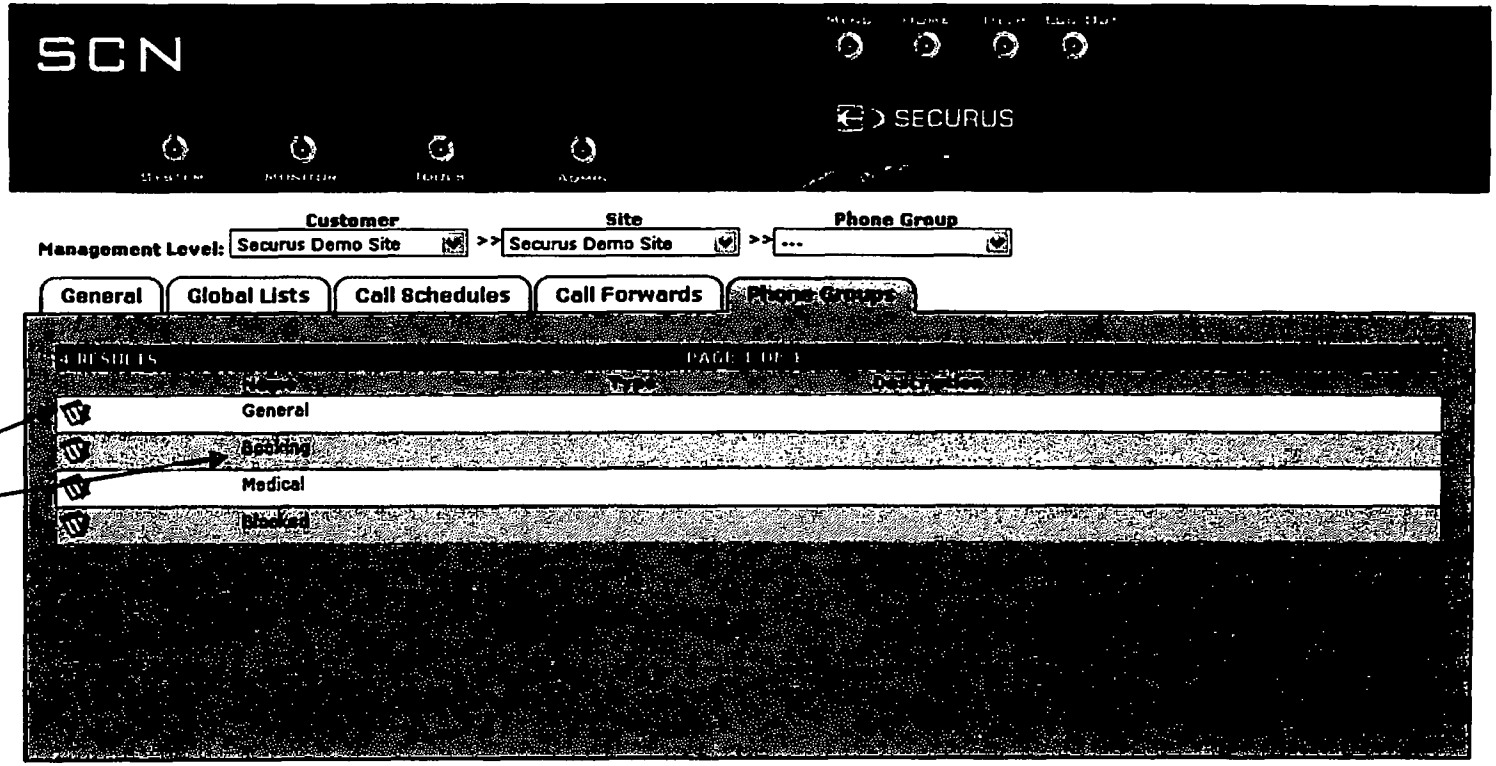
Call Forwards Setup Page is used to setup specific numbers to which a live call may be forwarded to for remote monitoring by authorized personnel.

Call Forwards Editor



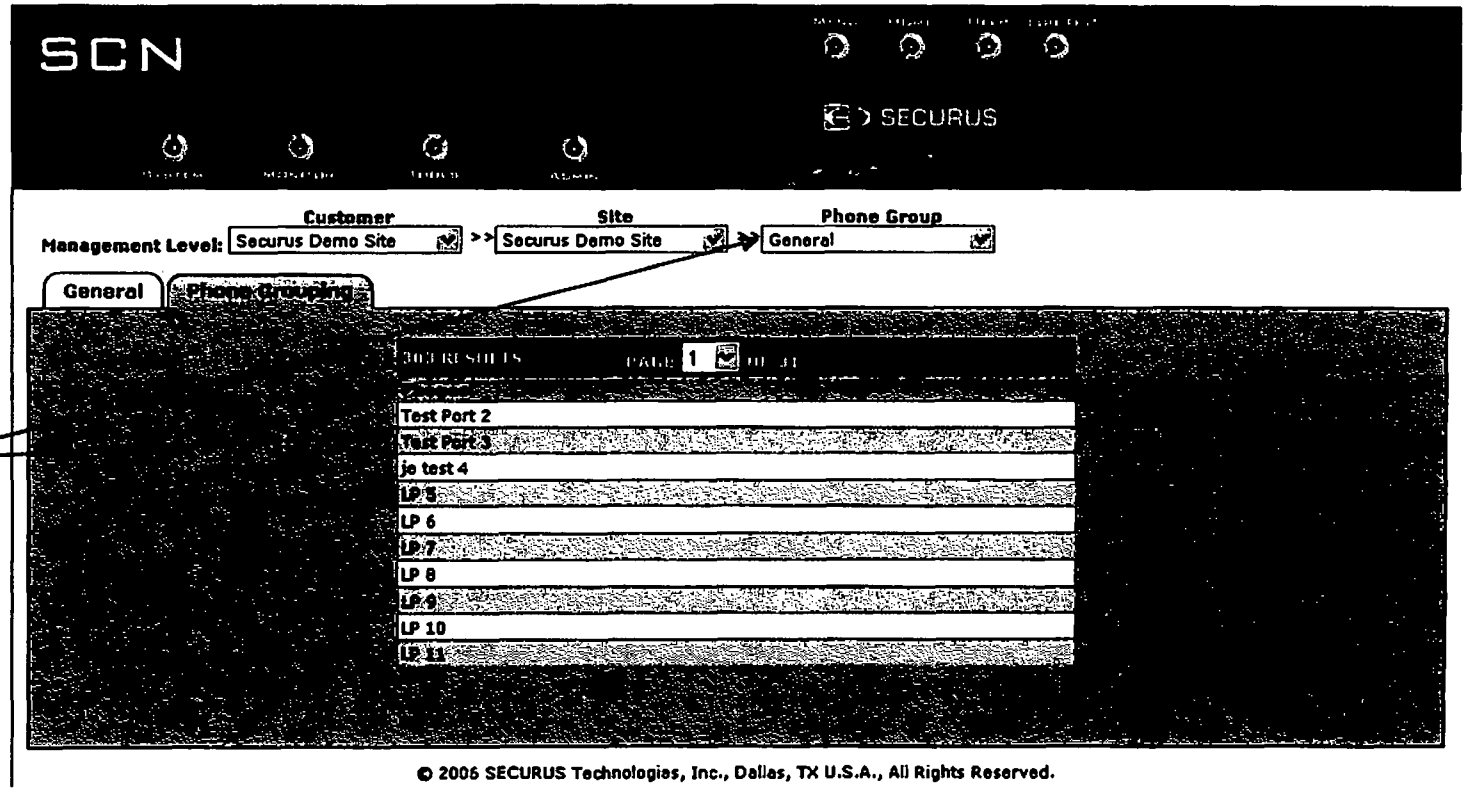
Call Forwards Editor Page is used to remove selected old numbers from the call forwards list.

Phone Group Screen



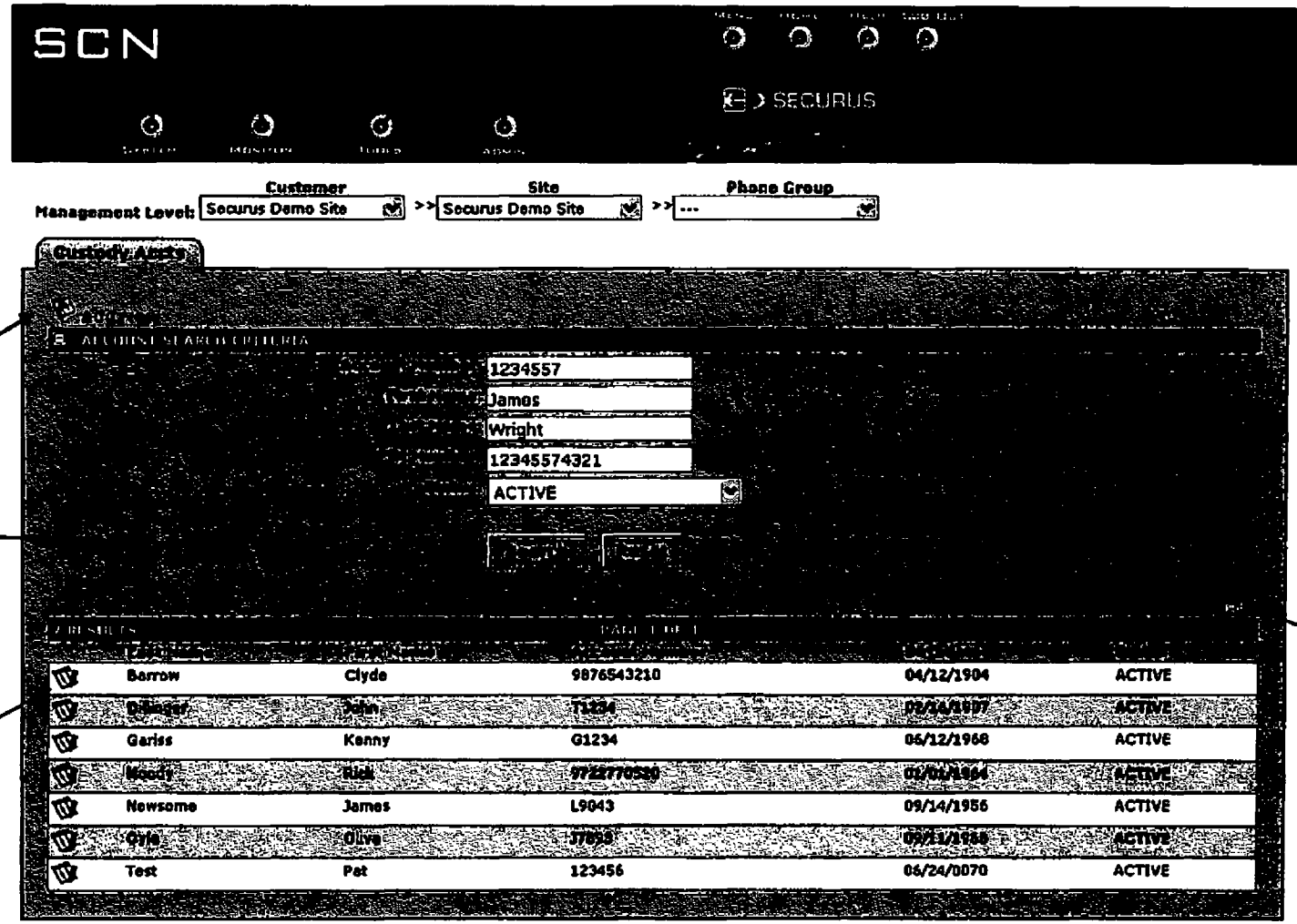
Phone Group Page is used by site administrators or authorized users to view and or modify the call schedule for one or multiple phone groups.

Phone Grouping Editor Screen



Phone Grouping Editor Page is used by site administrators or authorized users to view phones assigned to a selected phone group.

Custody Account Screen



Set up new custody accounts

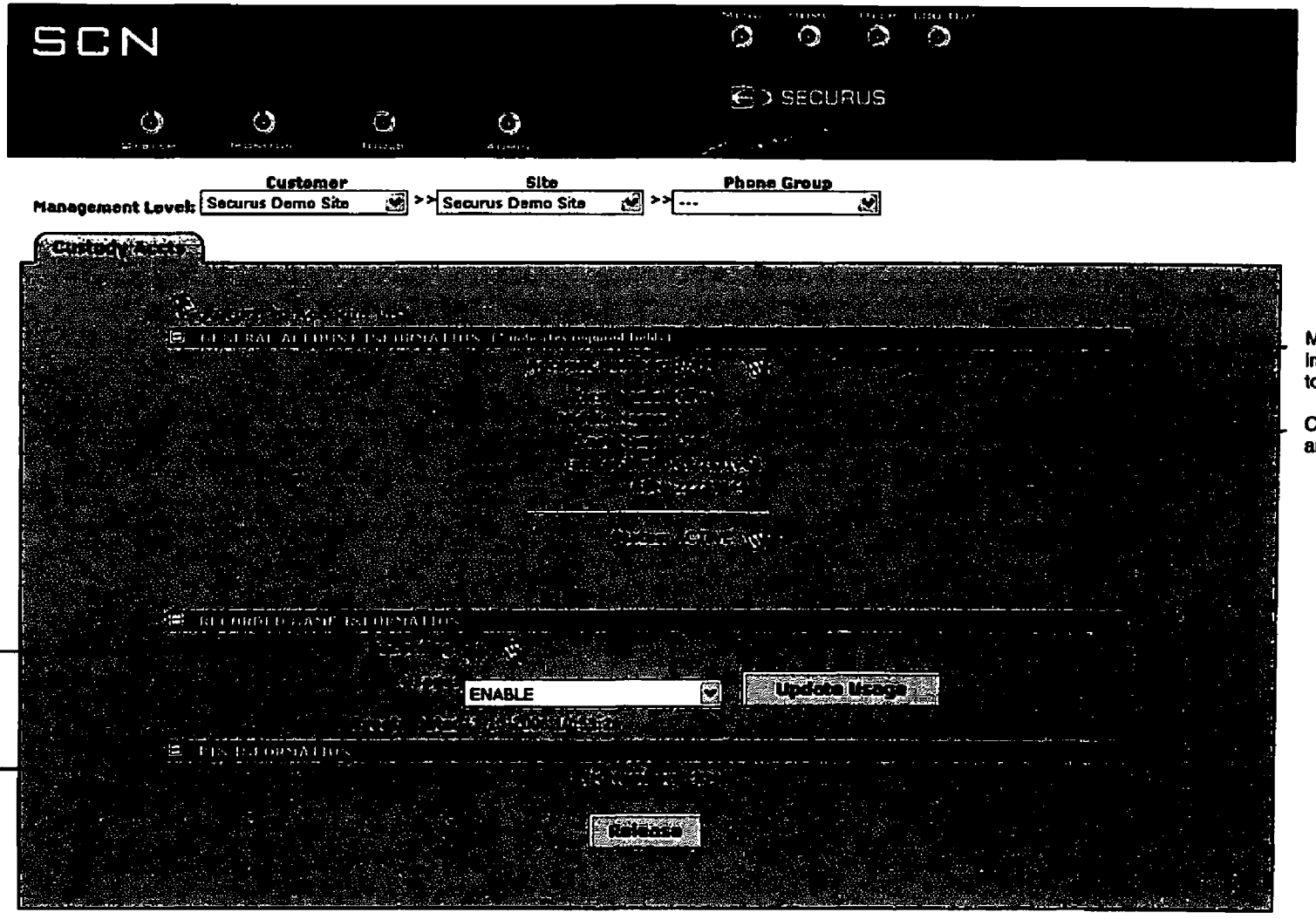
Search the site database for an existing account

Edit and modify an existing account

View and print an alpha list of all accounts in PDF format

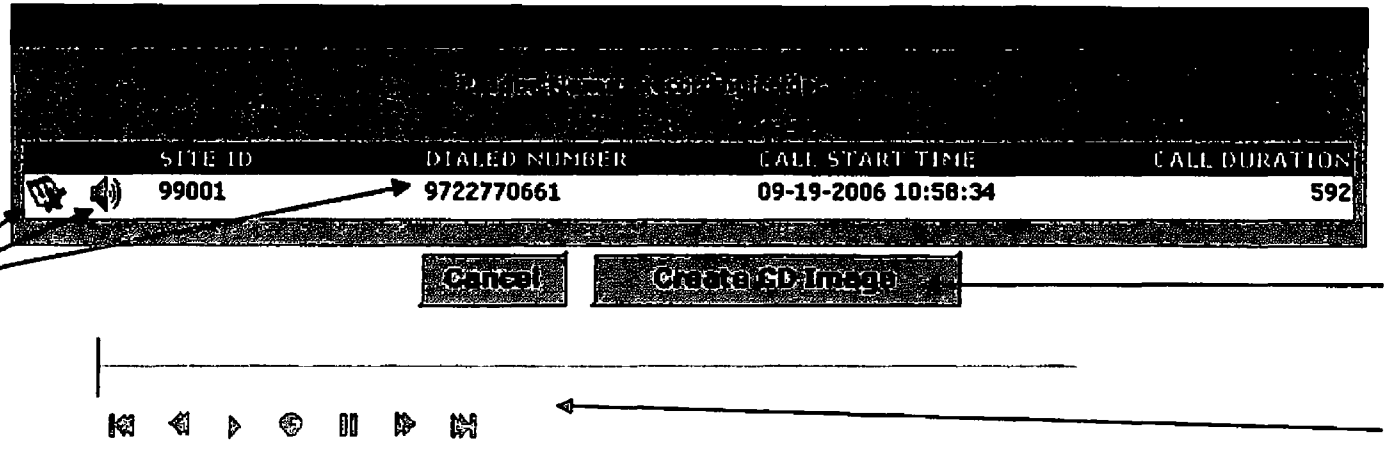
Custody Account Page is used by site administrators or authorized users to set up new accounts, search for existing records or modify the status and or information pertaining to a selected custody account.

Custody Account Editor



Custody Account Editor Page is used by site administrators or authorized users to modify personal information relative to an account, delete and re-record name information, and remove or release PIN information for inactive accounts.

Create CD Image Screen

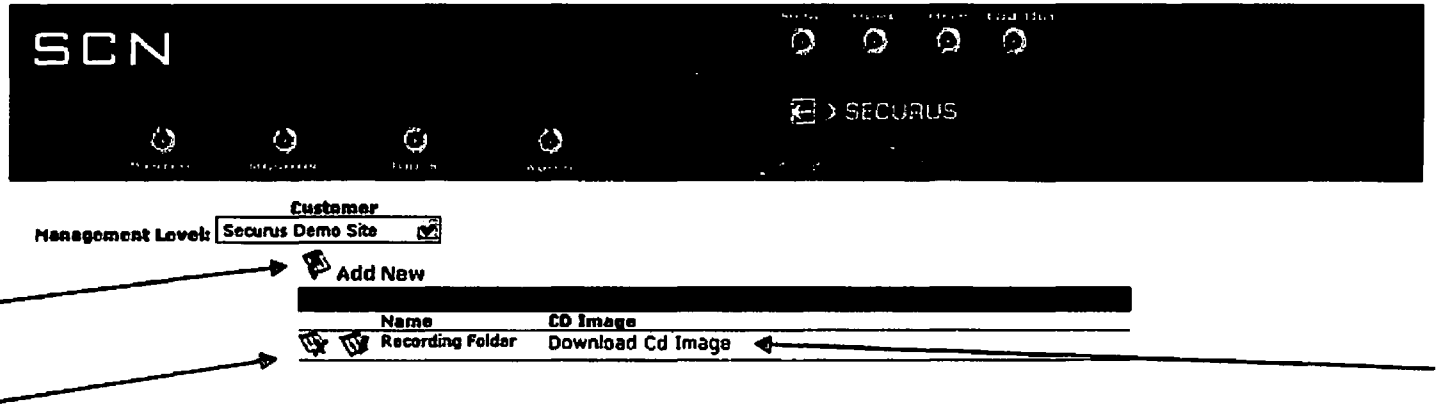


View or remove call detail record or listen to the call in the CD recording folder.

Click here to create a CD image of call records in the CD folder.

Media player for playing and listening to calls.

Download & Burn CD Screen



Create a new recording folder

Delete an existing recording folder

Download and burn image to CD disc.

CD Download & Burn Page is used by site administrators and authorized users to copy selected call detail records to a specific CD folder, create a CD image, and burn CD image to CD disc.

Sample Call Detail Report

Management Level: Customer: Securus Demo Site >> Site: Securus Demo Site >> Phone Group: ---

Call Detail Records Search

View Criteria

PDF

6 RESULTS — PAGE 1 OF 1

	Play	Site	Port Loc	Dialed Number	Start Date/Time	End Date/Time	Dur. (s)	Acct#	PIN	First Name	Last Name	Call Type	Call Status	Term. Category	Priv.	Watched	Int'l
☐	🔊	Securus Demo Site		9722770548	09-11-2006 11:03:00	09-11-2006 11:03:13	13					Person Call	complete	Inmate Hung-Up			
☐	🔊	Securus Demo Site		9722770548	09-11-2006 11:40:51	09-11-2006 11:40:59	8					Person Call	complete	Inmate Hung-Up			
☐	🔊	Securus Demo Site		9722770414	09-11-2006 17:01:50	09-11-2006 17:01:55	5					Person Call	complete	Inmate Hung-Up			
☐	🔊	Securus Demo Site		9722770665	09-11-2006 19:07:31	09-11-2006 19:09:03	92					Person Call	complete	Inmate Hung-Up			
☐	🔊	Securus Demo Site		9722770632	09-11-2006 20:35:16	09-11-2006 20:36:21	65					Person Call	complete	Inmate Hung-Up			
☐	🔊	Securus Demo Site		9722770665	09-11-2006 20:37:59	09-11-2006 20:38:01	2					Person Call	complete	Inmate Hung-Up			

Listen to recorded calls

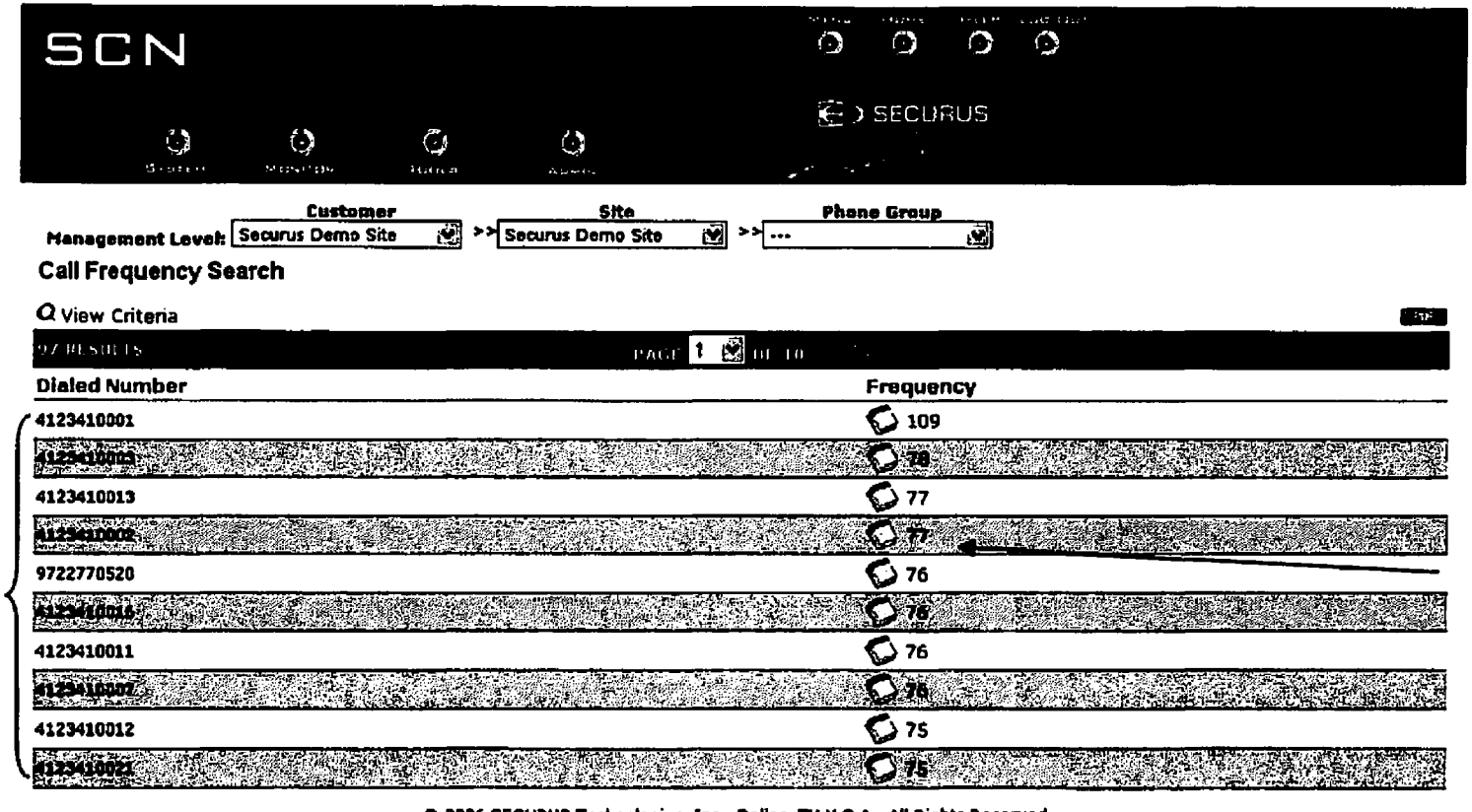
Select one or more call detail records to save to a CD folder

Click here to save selected call detail records to a CD folder

Print a PDF copy of call detail report

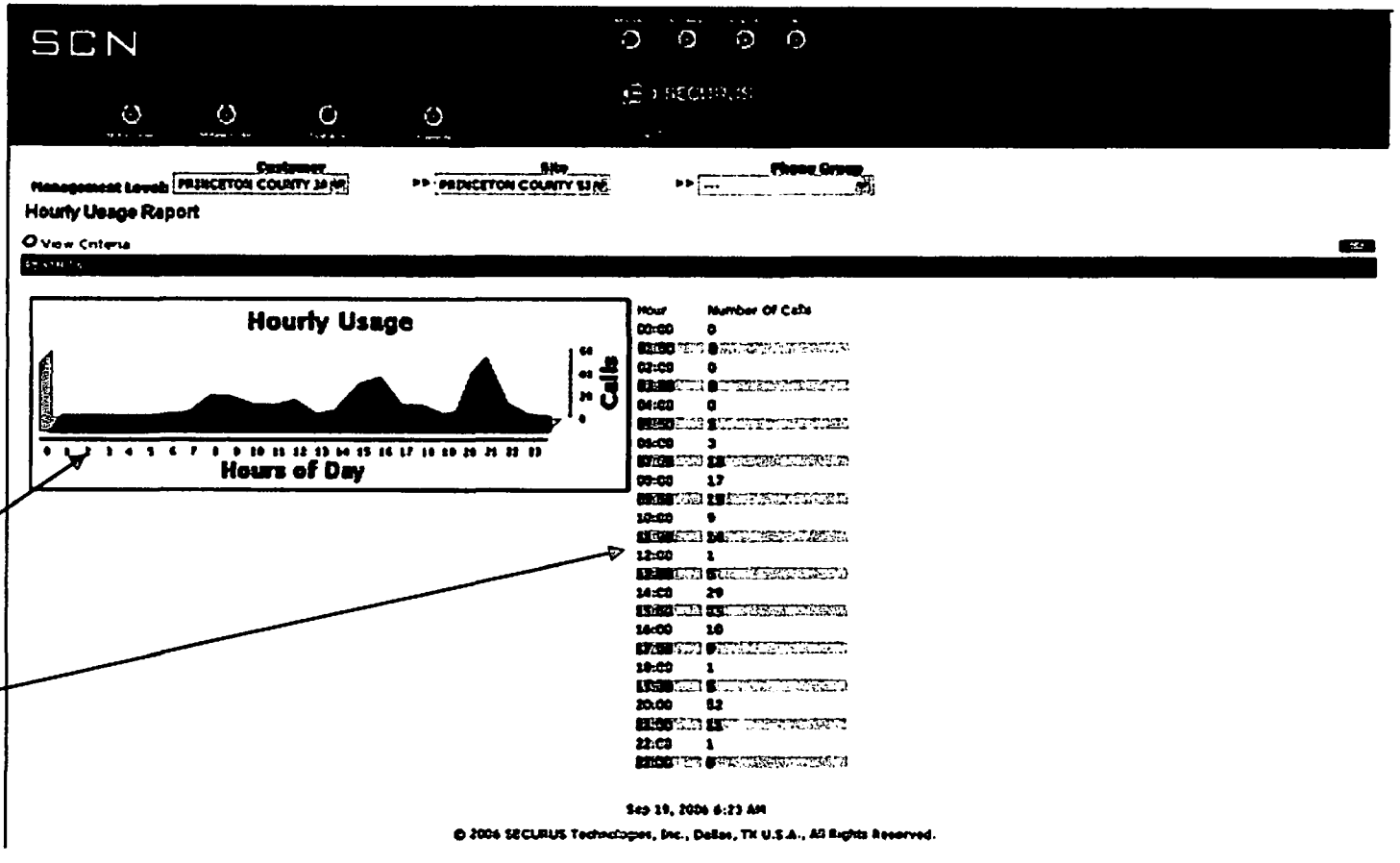
Call Detail Search Results Page is used by authorized users to view selected call detail records, playback and listen to selected calls, and select and save call detail records to a CD folder.

Sample Call Frequency Report



Global Lists Setup Page is used to configure dialing access to called party numbers. On this page users may configure whether or not a called number is blocked or private, and also gives users the ability to enter a speed dial code for the number.

Sample Hourly Usage Report



View report graph depicting peak calling times during the day

View hourly calling trends

Hourly Usage Report Page is used by authorized users to view a report graph of peaks and lows in hourly calling trends. Graph can also be used to view calls made outside of the authorized calling times.

Sample Blocked Call Detail Report

Management Level: Customer: Securus Demo Site >> Site: --- >> Phone Group: ---

Block Call Search

View Criteria

2 RESULTS PAGE 1 OF 1

Site	Port Loc	Dialed Number	Start Date/Time	End Date/Time	Dur. (s)	Acct#	PIN	First Name	Last Name	Call Type	Block Reason
Securus Demo Site	LP 26	4123410277	01-10-2007 01:47:13	01-10-2007 01:47:38	0	J7898	1234	Olive	Oyle	Person Call	No billing arrangement
Securus Demo Site	LP 26	[illegible]	01-10-2007 01:[illegible]	01-10-2007 01:[illegible]	0	J7898	1234	Olive	Oyle	Person Call	Invalid number dialed

Display search criteria screen to generate a new report

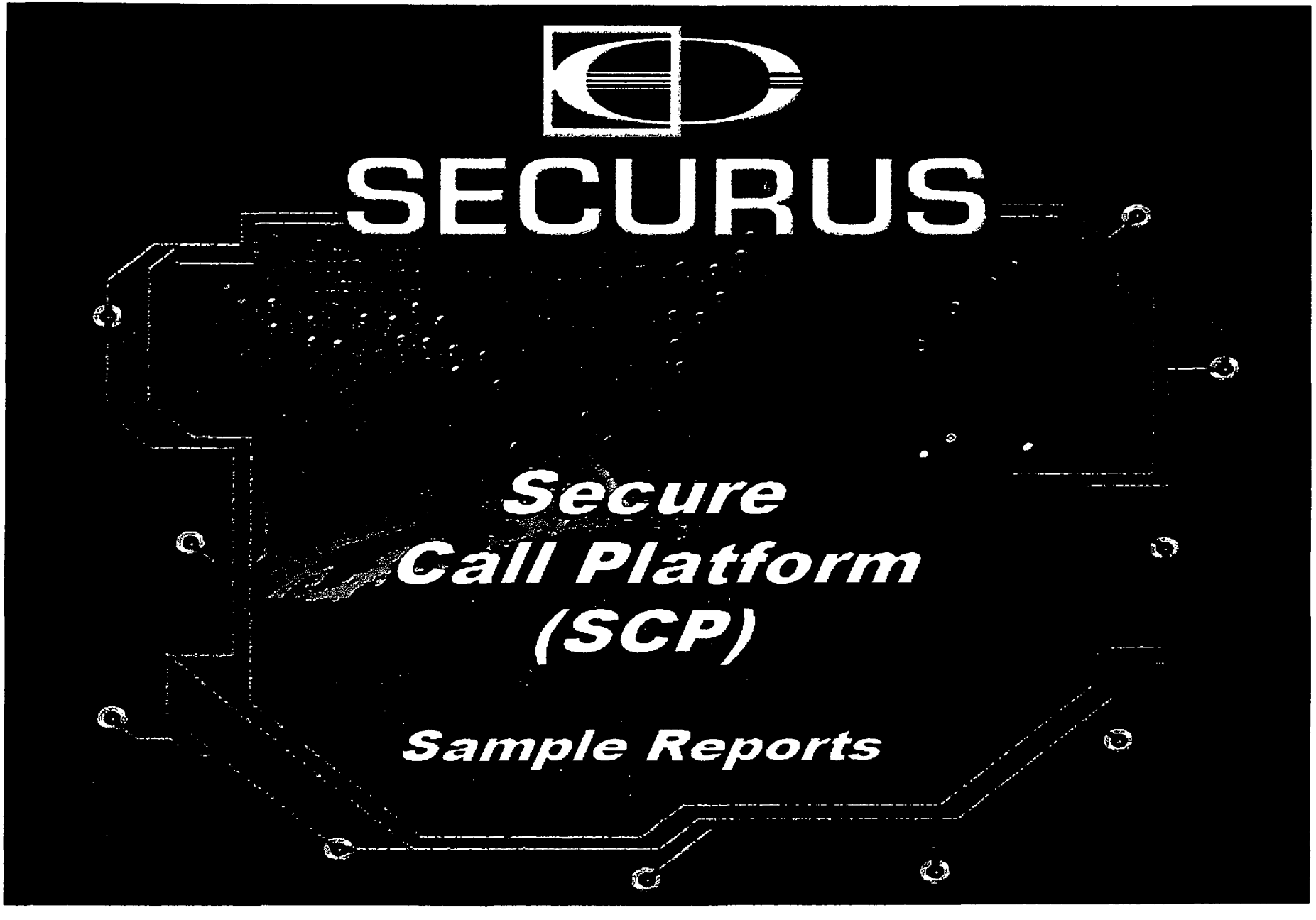
View the reason calls to a selected dialed number was not completed.

Blocked Call Detail Report Page is used by authorized users to review call detail report to determine why calls to the selected phone numbers were not completed successfully.

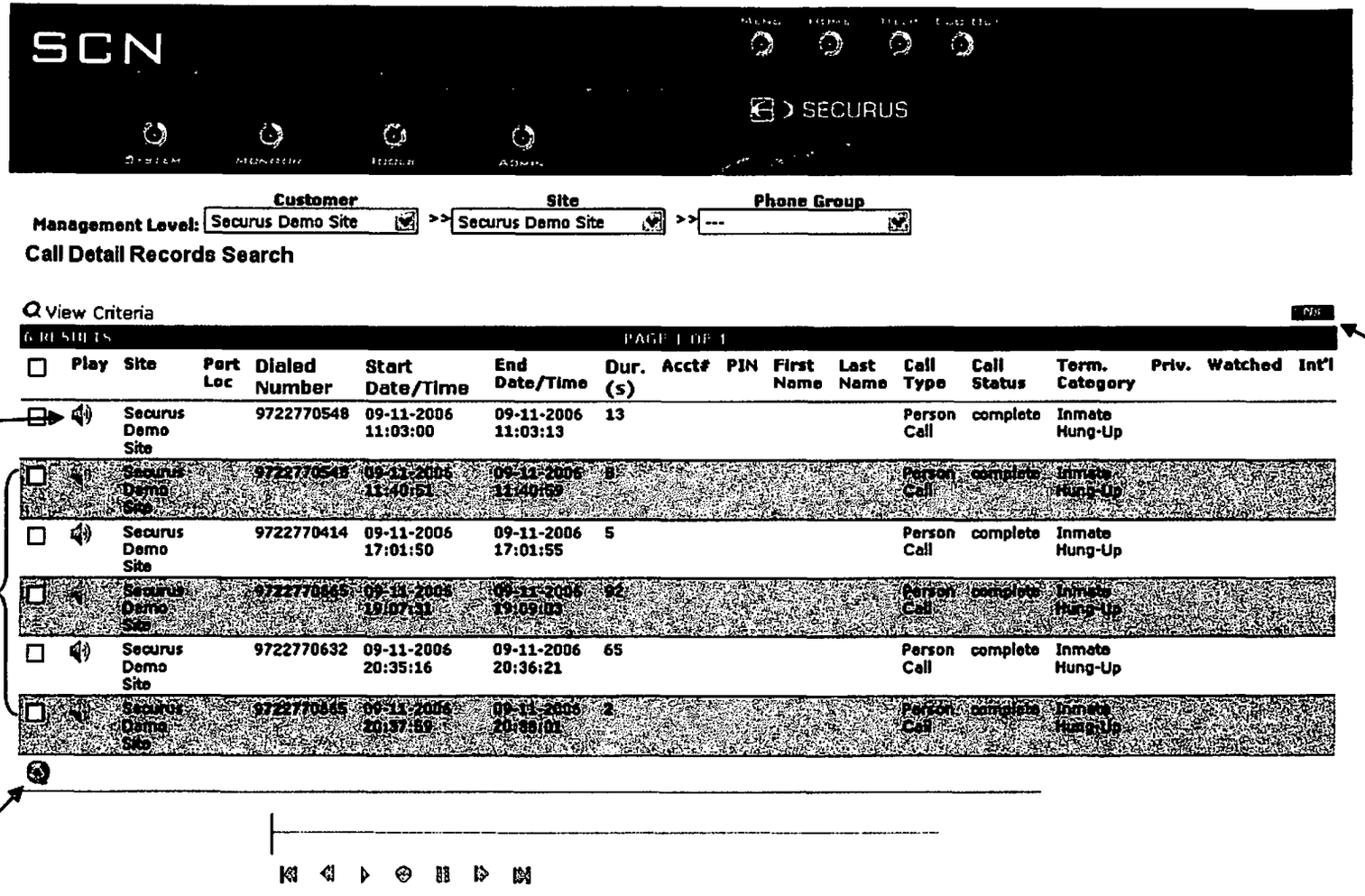
Page intentionally left blank

Attachment G

SECURUS Sample Reports

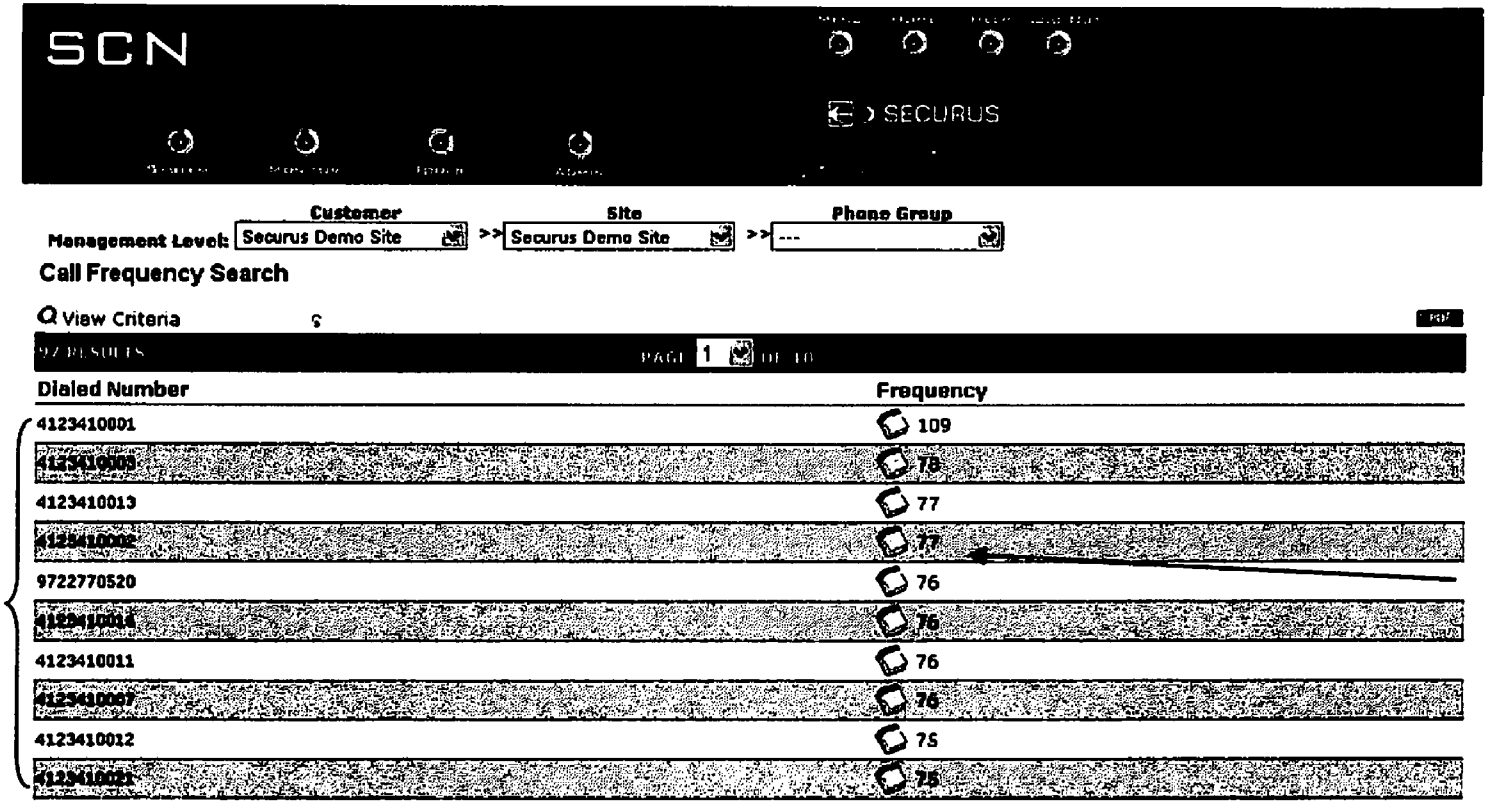


Sample Call Detail Report



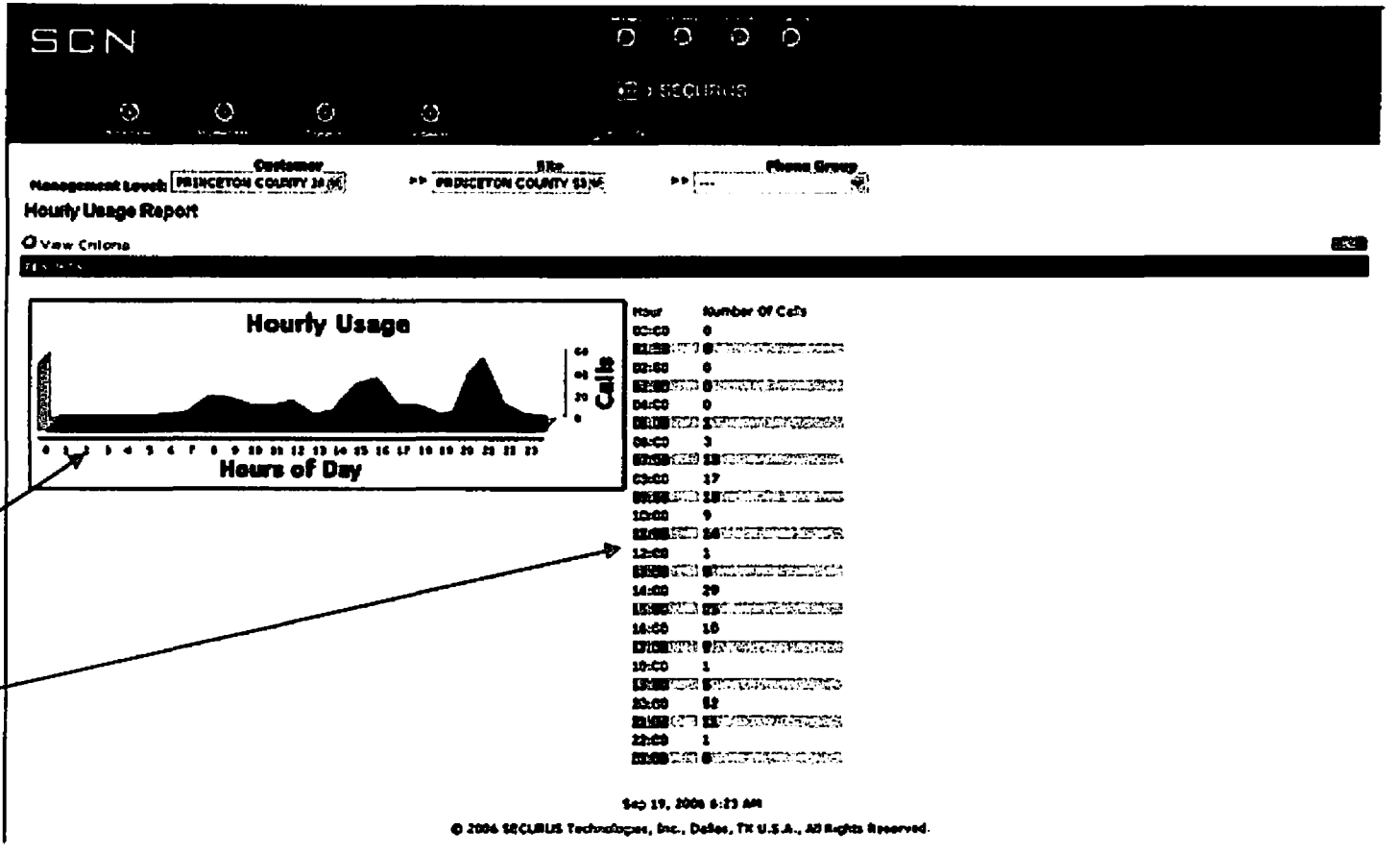
Call Detail Search Results Page is used by authorized users to view selected call detail records, playback and listen to selected calls, and select and save call detail records to a CD folder.

Sample Call Frequency Report



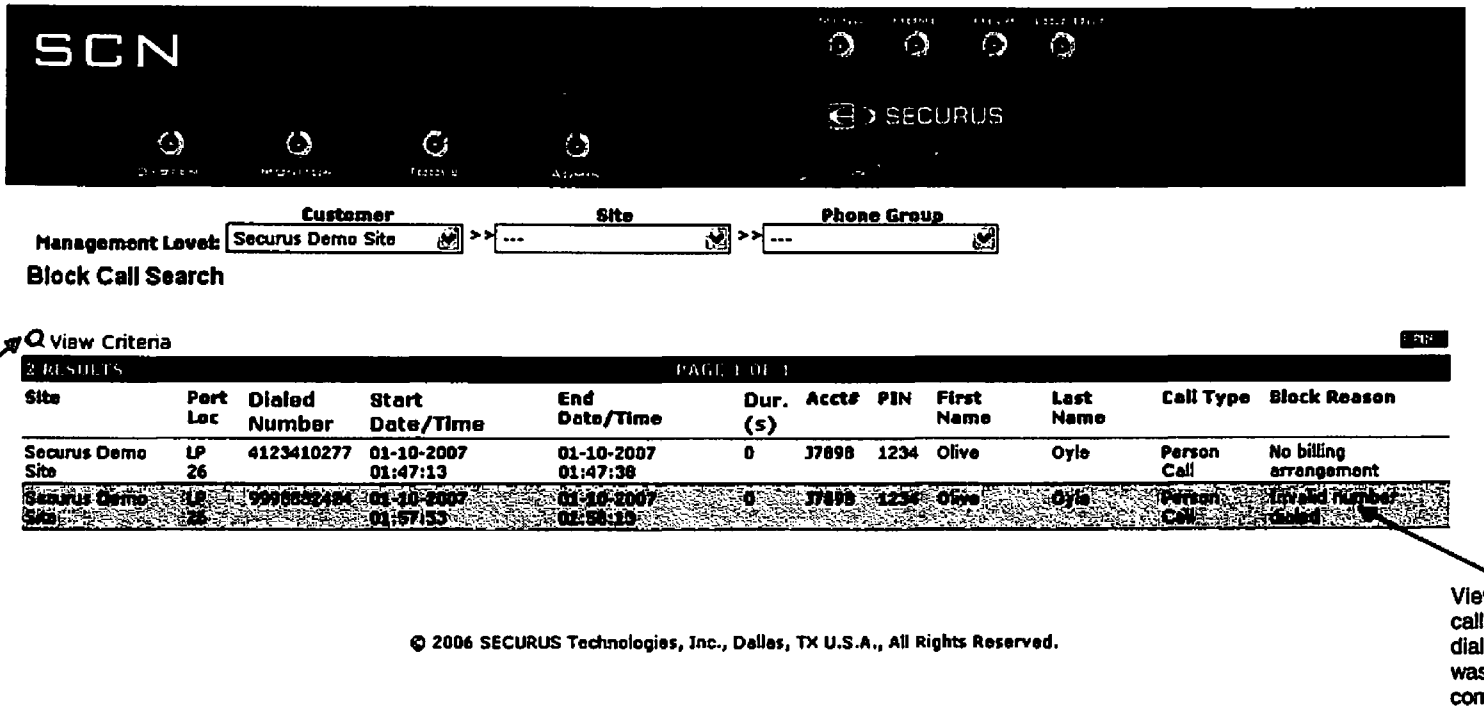
Global Lists Setup Page is used to configure dialing access to called party numbers. On this page users may configure whether or not a called number is blocked or private, and also gives users the ability to enter a speed dial code for the number.

Sample Hourly Usage Report



Hourly Usage Report Page is used by authorized users to view a report graph of peaks and lows in hourly calling trends. Graph can also be used to view calls made outside of the authorized calling times.

Sample Blocked Call Detail Report



Blocked Call Detail Report Page is used by authorized users to review call detail report to determine why calls to the selected phone numbers were not completed successfully.

Page intentionally left blank

Attachment H

SECURUS Preliminary Project Plan

ID	Task Name	Duration	Start	Finish	Predecessors	Resources
1	**ALASKA DOC**	**28 days**	**Mon 3/3/08**	**Wed 4/9/08**		
2	**Kickoff Meeting**	1 day	Mon 3/3/08	Mon 3/3/08		Project Team & County Personnel
3	Confirm Install dates, Shipping, & Training	8 hrs	Mon 3/3/08	Mon 3/3/08		
4	**Weekly Conference Calls**	**28 days**	**Mon 3/3/08**	**Wed 4/9/08**		
5	Status Updates, Issues, etc....	28 days	Mon 3/3/08	Wed 4/9/08		
6	**Pre-Install Activities - ALASKA DOC**	**1 day**	**Mon 3/3/08**	**Mon 3/3/08**		
7	Order/Install Lines for all locations	1 day	Mon 3/3/08	Mon 3/3/08		T-1,MPLS,CO's
8	Feature Selection Confirmed	0 days	Mon 3/3/08	Mon 3/3/08		
9	Obtain Line Numbers & Confirm Orders and Due Dates with LEC	0 days	Mon 3/3/08	Mon 3/3/08	8	
10	Branding Messages Developed	0 days	Mon 3/3/08	Mon 3/3/08	9	
11	Pull Equipment & Parts	0 days	Mon 3/3/08	Mon 3/3/08		
12	Build Inmate Call Out Program	0 days	Mon 3/3/08	Mon 3/3/08	10	
13	Configure Inmate Call Out Program	0 days	Mon 3/3/08	Mon 3/3/08	11	
14	Quality Control IPS test	0 days	Mon 3/3/08	Mon 3/3/08	13	Feature,System,& Load testing
15						
16	**Install Activities - Anchorage - 98 phones**	**12.5 days**	**Mon 3/3/08**	**Wed 3/19/08**		Team 1 - 2 Techs
17	**Receipt & General Install Tasks**	**7.5 days**	**Mon 3/3/08**	**Wed 3/12/08**		
18	Travel to site	0.5 days	Mon 3/3/08	Mon 3/3/08		
19	Receive System Shipment at Site	0 days	Mon 3/3/08	Mon 3/3/08	18	
20	Verify Shipment Content to Pick List	2 hrs	Mon 3/3/08	Mon 3/3/08		
21	Survey site	4 hrs	Mon 3/3/08	Mon 3/3/08		
22	General Installation - System, phones (including cut-off switches)	7 days	Mon 3/3/08	Wed 3/12/08	21	
23	**Test & Turn Up of Circuits on Site with LEC**	**0.5 days**	**Mon 3/3/08**	**Mon 3/3/08**		
24	Test & Turn Up Circuits	2 hrs	Mon 3/3/08	Mon 3/3/08		
25	Circuits Active/Ready	2 hrs	Mon 3/3/08	Mon 3/3/08	24	
26	**Cutover Tasks**	**4.5 days**	**Thu 3/13/08**	**Wed 3/19/08**		
27	**Cutover, Test & Quality Check (QC) Tasks**	**4.5 days**	**Thu 3/13/08**	**Wed 3/19/08**		
28	Verify all Features working properly	0.5 days	Thu 3/13/08	Thu 3/13/08		
29	Verify phones work, port assignments/call groups set	4 days	Thu 3/13/08	Tue 3/18/08		
30	QC Checklist & Test Calls Completed	0.5 days	Wed 3/19/08	Wed 3/19/08		
31	**Cut Sheet & QC Workbook Completed**	**0.25 days**	**Wed 3/19/08**	**Wed 3/19/08**		
32	Site Cutover to New System	0 days	Wed 3/19/08	Wed 3/19/08		
33	Distribute Cut Sheet to Logistics Planning	1 hr	Wed 3/19/08	Wed 3/19/08		
34	Site Cutover Complete - Ready for Training	0 days	Wed 3/19/08	Wed 3/19/08	33	
35	Workstation & Firewall (If Required)	2 hrs	Wed 3/19/08	Wed 3/19/08		
36	**Training - Anchorage - 98 phones**	**1 day**	**Thu 3/20/08**	**Thu 3/20/08**		TRAINING
37	Perform Customer Training	1 day	Thu 3/20/08	Thu 3/20/08		
38	Complete Training Sign Off Including Heat Ticket	1 hr	Thu 3/20/08	Thu 3/20/08		
39						
40	**Install Activities - Anvil Mountain - 11 phones**	**3.5 days**	**Mon 3/3/08**	**Thu 3/6/08**		Team 2 - 2 Techs

Project: Alaska DOC
Date: Tue 1/15/08

Critical	Progress	Summary	External Tasks		
Critical Split	Milestone	Project Summary	External Milestone		
Task	Slack	Rolled Up Critical	Deadline		
Split	Slippage	Rolled Up Critical Split			

ID	Task Name	Duration	Start	Finish	Predecessors	Resources
41	**Receipt & General Install Tasks**	**1.25 days**	**Mon 3/3/08**	**Tue 3/4/08**		
42	Travel to site	0.5 days	Mon 3/3/08	Mon 3/3/08		
43	Receive System Shipment at Site	0 days	Mon 3/3/08	Mon 3/3/08	42	
44	Verify Shipment Content to Pick List	2 hrs	Mon 3/3/08	Mon 3/3/08		
45	Survey site	2 hrs	Mon 3/3/08	Mon 3/3/08		
46	General Installation - System, phones (including cut-off switches)	1 day	Mon 3/3/08	Tue 3/4/08	45	
47	**Test & Turn Up of Circuits on Site with LEC**	**0.5 days**	**Mon 3/3/08**	**Mon 3/3/08**		
48	Test & Turn Up Circuits	2 hrs	Mon 3/3/08	Mon 3/3/08		
49	Circuits Active/Ready	2 hrs	Mon 3/3/08	Mon 3/3/08	48	
50	**Cutover Tasks**	**1.5 days**	**Wed 3/5/08**	**Thu 3/6/08**		
51	**Cutover, Test & Quality Check (QC) Tasks**	**1.5 days**	**Wed 3/5/08**	**Thu 3/6/08**		
52	Verify all Features working properly	0.5 days	Wed 3/5/08	Wed 3/5/08		
53	Verify phones work, port assignments/call groups set	1 day	Wed 3/5/08	Wed 3/5/08		
54	QC Checklist & Test Calls Completed	0.5 days	Thu 3/6/08	Thu 3/6/08		
55	**Cut Sheet & QC Workbook Completed**	**0.25 days**	**Thu 3/6/08**	**Thu 3/6/08**		
56	Site Cutover to New System	0 days	Thu 3/6/08	Thu 3/6/08		
57	Distribute Cut Sheet to Logistics Planning	1 hr	Thu 3/6/08	Thu 3/6/08		
58	Site Cutover Complete - Ready for Training	0 days	Thu 3/6/08	Thu 3/6/08	57	
59	Workstation & Firewall (If Required)	2 hrs	Thu 3/6/08	Thu 3/6/08		
60	**Training - Anvil Mountain - 11 phones**	**1 day**	**Fri 3/7/08**	**Fri 3/7/08**		**TRAINING**
61	Perform Customer Training	1 day	Fri 3/7/08	Fri 3/7/08		
62	Complete Training Sign Off Including Heat Ticket	1 hr	Fri 3/7/08	Fri 3/7/08		
63						
64	**Install Activities - Fairbanks - 38 phones**	**8.25 days**	**Mon 3/10/08**	**Thu 3/20/08**		**Team 2 - 2 Techs**
65	**Receipt & General Install Tasks**	**3.5 days**	**Mon 3/10/08**	**Thu 3/13/08**		
66	Travel to site	0.5 days	Mon 3/10/08	Mon 3/10/08		
67	Receive System Shipment at Site	0 days	Mon 3/10/08	Mon 3/10/08	66	
68	Verify Shipment Content to Pick List	2 hrs	Mon 3/10/08	Mon 3/10/08		
69	Survey site	4 hrs	Mon 3/10/08	Mon 3/10/08		
70	General Installation - System, phones (including cut-off switches)	3 days	Mon 3/10/08	Thu 3/13/08	69	
71	**Test & Turn Up of Circuits on Site with LEC**	**0.5 days**	**Mon 3/10/08**	**Mon 3/10/08**		
72	Test & Turn Up Circuits	2 hrs	Mon 3/10/08	Mon 3/10/08		
73	Circuits Active/Ready	2 hrs	Mon 3/10/08	Mon 3/10/08	72	
74	**Cutover Tasks**	**5.25 days**	**Thu 3/13/08**	**Thu 3/20/08**		
75	**Cutover, Test & Quality Check (QC) Tasks**	**4.5 days**	**Thu 3/13/08**	**Wed 3/19/08**		
76	Verify all Features working properly	0.5 days	Thu 3/13/08	Thu 3/13/08		
77	Verify phones work, port assignments/call groups set	4 days	Thu 3/13/08	Tue 3/18/08		
78	QC Checklist & Test Calls Completed	0.5 days	Wed 3/19/08	Wed 3/19/08		
79	**Cut Sheet & QC Workbook Completed**	**0.25 days**	**Thu 3/20/08**	**Thu 3/20/08**		
80	Site Cutover to New System	0 days	Thu 3/20/08	Thu 3/20/08		

Project: Alaska DOC
Date: Tue 1/15/08

Critical
Critical Split
Task
Split
Progress
Milestone
Slack
Slippage
Summary
Project Summary
Rolled Up Critical
Rolled Up Critical Split
External Tasks
External Milestone
Deadline

ID	Task Name	Duration	Start	Finish	Predecessors	Resources	S
81	Distribute Cut Sheet to Logistics Planning	1 hr	Thu 3/20/08	Thu 3/20/08			
82	Site Cutover Complete - Ready for Training	0 days	Thu 3/20/08	Thu 3/20/08	81		
83	Workstation & Firewall (If Required)	2 hrs	Thu 3/20/08	Thu 3/20/08			
84	**Training - Fairbanks - 38 phones**	**1 day**	**Fri 3/21/08**	**Fri 3/21/08**		**TRAINING**	
85	Perform Customer Training	1 day	Fri 3/21/08	Fri 3/21/08			
86	Complete Training Sign Off Including Heat Ticket	1 hr	Fri 3/21/08	Fri 3/21/08			
87							
88	**Install Activities - Hiland Mountain - 28 phones**	**5 days**	**Fri 3/21/08**	**Thu 3/27/08**		**Team 1 - 2 Techs**	
89	**Receipt & General Install Tasks**	**2.5 days**	**Fri 3/21/08**	**Tue 3/25/08**			
90	Travel to site	0.5 days	Fri 3/21/08	Fri 3/21/08			
91	Receive System Shipment at Site	0 days	Fri 3/21/08	Fri 3/21/08	90		
92	Verify Shipment Content to Pick List	2 hrs	Fri 3/21/08	Fri 3/21/08			
93	Survey site	4 hrs	Fri 3/21/08	Fri 3/21/08			
94	General Installation - System, phones (including cut-off switches)	2 days	Fri 3/21/08	Tue 3/25/08	93		
95	**Test & Turn Up of Circuits on Site with LEC**	**0.5 days**	**Fri 3/21/08**	**Fri 3/21/08**			
96	Test & Turn Up Circuits	2 hrs	Fri 3/21/08	Fri 3/21/08			
97	Circuits Active/Ready	2 hrs	Fri 3/21/08	Fri 3/21/08	96		
98	**Cutover Tasks**	**2 days**	**Wed 3/26/08**	**Thu 3/27/08**			
99	**Cutover, Test & Quality Check (QC) Tasks**	**2 days**	**Wed 3/26/08**	**Thu 3/27/08**			
100	Verify all Features working properly	0.5 days	Wed 3/26/08	Wed 3/26/08			
101	Verify phones work, port assignments/call groups set	2 days	Wed 3/26/08	Thu 3/27/08			
102	QC Checklist & Test Calls Completed	0.5 days	Thu 3/27/08	Thu 3/27/08			
103	**Cut Sheet & QC Workbook Completed**	**0.25 days**	**Thu 3/27/08**	**Thu 3/27/08**			
104	Site Cutover to New System	0 days	Thu 3/27/08	Thu 3/27/08			
105	Distribute Cut Sheet to Logistics Planning	1 hr	Thu 3/27/08	Thu 3/27/08			
106	Site Cutover Complete - Ready for Training	0 days	Thu 3/27/08	Thu 3/27/08	105		
107	Workstation & Firewall (If Required)	2 hrs	Thu 3/27/08	Thu 3/27/08			
108	**Training - Hiland Mountain - 28 phones**	**1 day**	**Fri 3/28/08**	**Fri 3/28/08**		**TRAINING**	
109	Perform Customer Training	1 day	Fri 3/28/08	Fri 3/28/08			
110	Complete Training Sign Off Including Heat Ticket	1 hr	Fri 3/28/08	Fri 3/28/08			
111							
112	**Install Activities - Ketchikan - 6 phones**	**3.5 days**	**Mon 3/3/08**	**Thu 3/6/08**		**Team 3 - 2 Techs**	
113	**Receipt & General Install Tasks**	**1.5 days**	**Mon 3/3/08**	**Tue 3/4/08**			
114	Travel to site	0.5 days	Mon 3/3/08	Mon 3/3/08			
115	Receive System Shipment at Site	0 days	Mon 3/3/08	Mon 3/3/08	114		
116	Verify Shipment Content to Pick List	2 hrs	Mon 3/3/08	Mon 3/3/08			
117	Survey site	4 hrs	Mon 3/3/08	Mon 3/3/08			
118	General Installation - System, phones (including cut-off switches)	1 day	Mon 3/3/08	Tue 3/4/08	117		
119	**Test & Turn Up of Circuits on Site with LEC**	**0.5 days**	**Mon 3/3/08**	**Mon 3/3/08**			
120	Test & Turn Up Circuits	2 hrs	Mon 3/3/08	Mon 3/3/08			

Project: Alaska DOC
Date: Tue 1/15/08

Critical	Progress	Summary	External Tasks		
Critical Split	Milestone	Project Summary	External Milestone		
Task	Slack	Rolled Up Critical	Deadline		
Split	Slippage	Rolled Up Critical Split			

ID	Task Name	Duration	Start	Finish	Predecessors	Resources
121	Circuits Active/Ready	2 hrs	Mon 3/3/08	Mon 3/3/08	120	
122	**Cutover Tasks**	**1.5 days**	**Wed 3/5/08**	**Thu 3/6/08**		
123	**Cutover, Test & Quality Check (QC) Tasks**	**1.5 days**	**Wed 3/5/08**	**Thu 3/6/08**		
124	Verify all Features working properly	0.5 days	Wed 3/5/08	Wed 3/5/08		
125	Verify phones work, port assignments/call groups set	0.5 days	Wed 3/5/08	Wed 3/5/08		
126	QC Checklist & Test Calls Completed	0.5 days	Thu 3/6/08	Thu 3/6/08		
127	**Cut Sheet & QC Workbook Completed**	**0.25 days**	**Thu 3/6/08**	**Thu 3/6/08**		
128	Site Cutover to New System	0 days	Thu 3/6/08	Thu 3/6/08		
129	Distribute Cut Sheet to Logistics Planning	1 hr	Thu 3/6/08	Thu 3/6/08		
130	Site Cutover Complete - Ready for Training	0 days	Thu 3/6/08	Thu 3/6/08	129	
131	Workstation & Firewall (If Required)	2 hrs	Thu 3/6/08	Thu 3/6/08		
132	**Training - Ketchikan - 6 phones**	**1 day**	**Fri 3/7/08**	**Fri 3/7/08**		**TRAINING**
133	Perform Customer Training	1 day	Fri 3/7/08	Fri 3/7/08		
134	Complete Training Sign Off Including Heat Ticket	1 hr	Fri 3/7/08	Fri 3/7/08		
135						
136	**Install Activities - Lemon Creek - 45 phones**	**6.25 days**	**Mon 3/31/08**	**Tue 4/8/08**		**Team 1 - 2 Techs**
137	**Receipt & General Install Tasks**	**3.5 days**	**Mon 3/31/08**	**Thu 4/3/08**		
138	Travel to site	0.5 days	Mon 3/31/08	Mon 3/31/08		
139	Receive System Shipment at Site	0 days	Mon 3/31/08	Mon 3/31/08	138	
140	Verify Shipment Content to Pick List	2 hrs	Mon 3/31/08	Mon 3/31/08		
141	Survey site	4 hrs	Mon 3/31/08	Mon 3/31/08		
142	General Installation - System, phones (including cut-off switches)	3 days	Mon 3/31/08	Thu 4/3/08	141	
143	**Test & Turn Up of Circuits on Site with LEC**	**0.5 days**	**Mon 3/31/08**	**Mon 3/31/08**		
144	Test & Turn Up Circuits	2 hrs	Mon 3/31/08	Mon 3/31/08		
145	Circuits Active/Ready	2 hrs	Mon 3/31/08	Mon 3/31/08	144	
146	**Cutover Tasks**	**2.25 days**	**Fri 4/4/08**	**Tue 4/8/08**		
147	**Cutover, Test & Quality Check (QC) Tasks**	**2 days**	**Fri 4/4/08**	**Mon 4/7/08**		
148	Verify all Features working properly	0.5 days	Fri 4/4/08	Fri 4/4/08		
149	Verify phones work, port assignments/call groups set	1 day	Mon 4/7/08	Mon 4/7/08		
150	QC Checklist & Test Calls Completed	0.5 days	Mon 4/7/08	Mon 4/7/08		
151	**Cut Sheet & QC Workbook Completed**	**0.25 days**	**Tue 4/8/08**	**Tue 4/8/08**		
152	Site Cutover to New System	0 days	Tue 4/8/08	Tue 4/8/08		
153	Distribute Cut Sheet to Logistics Planning	1 hr	Tue 4/8/08	Tue 4/8/08		
154	Site Cutover Complete - Ready for Training	0 days	Tue 4/8/08	Tue 4/8/08	153	
155	Workstation & Firewall (If Required)	2 hrs	Tue 4/8/08	Tue 4/8/08		
156	**Training - Lemon Creek - 45 phones**	**1 day**	**Wed 4/9/08**	**Wed 4/9/08**		**TRAINING**
157	Perform Customer Training	1 day	Wed 4/9/08	Wed 4/9/08		
158	Complete Training Sign Off Including Heat Ticket	1 hr	Wed 4/9/08	Wed 4/9/08		
159						
160	**Install Activities - Matsu Pretrial - 12 phones**	**3.5 days**	**Mon 3/24/08**	**Thu 3/27/08**		**Team 2 - 2 Techs**

Project: Alaska DOC
Date: Tue 1/15/08

Critical
Critical Split
Task
Split
Progress
Milestone
Slack
Slippage
Summary
Project Summary
Rolled Up Critical
Rolled Up Critical Split
External Tasks
External Milestone
Deadline

ID	Task Name	Duration	Start	Finish	Predecessors	Resources
161	**Receipt & General Install Tasks**	**1.5 days**	**Mon 3/24/08**	**Tue 3/25/08**		
162	Travel to site	0.5 days	Mon 3/24/08	Mon 3/24/08		
163	Receive System Shipment at Site	0 days	Mon 3/24/08	Mon 3/24/08	162	
164	Verify Shipment Content to Pick List	2 hrs	Mon 3/24/08	Mon 3/24/08		
165	Survey site	4 hrs	Mon 3/24/08	Mon 3/24/08		
166	General Installation - System, phones (including cut-off switches)	1 day	Mon 3/24/08	Tue 3/25/08	165	
167	**Test & Turn Up of Circuits on Site with LEC**	**0.5 days**	**Mon 3/24/08**	**Mon 3/24/08**		
168	Test & Turn Up Circuits	2 hrs	Mon 3/24/08	Mon 3/24/08		
169	Circuits Active/Ready	2 hrs	Mon 3/24/08	Mon 3/24/08	168	
170	**Cutover Tasks**	**1.5 days**	**Wed 3/26/08**	**Thu 3/27/08**		
171	**Cutover, Test & Quality Check (QC) Tasks**	**1.5 days**	**Wed 3/26/08**	**Thu 3/27/08**		
172	Verify all Features working properly	0.5 days	Wed 3/26/08	Wed 3/26/08		
173	Verify phones work, port assignments/call groups set	0.5 days	Wed 3/26/08	Wed 3/26/08		
174	QC Checklist & Test Calls Completed	0.5 days	Thu 3/27/08	Thu 3/27/08		
175	**Cut Sheet & QC Workbook Completed**	**0.25 days**	**Thu 3/27/08**	**Thu 3/27/08**		
176	Site Cutover to New System	0 days	Thu 3/27/08	Thu 3/27/08		
177	Distribute Cut Sheet to Logistics Planning	1 hr	Thu 3/27/08	Thu 3/27/08		
178	Site Cutover Complete - Ready for Training	0 days	Thu 3/27/08	Thu 3/27/08	177	
179	Workstation & Firewall (If Required)	2 hrs	Thu 3/27/08	Thu 3/27/08		
180	**Training - Matsu Pretrial - 12 phones**	**1 day**	**Fri 3/28/08**	**Fri 3/28/08**		**TRAINING**
181	Perform Customer Training	1 day	Fri 3/28/08	Fri 3/28/08		
182	Complete Training Sign Off Including Heat Ticket	1 hr	Fri 3/28/08	Fri 3/28/08		
183						
184	**Install Activities - Palmer - 24 phones**	**5.5 days**	**Mon 3/10/08**	**Mon 3/17/08**		**Team 3 - 2 Techs**
185	**Receipt & General Install Tasks**	**2.5 days**	**Mon 3/10/08**	**Wed 3/12/08**		
186	Travel to site	0.5 days	Mon 3/10/08	Mon 3/10/08		
187	Receive System Shipment at Site	0 days	Mon 3/10/08	Mon 3/10/08		
188	Verify Shipment Content to Pick List	2 hrs	Mon 3/10/08	Mon 3/10/08		
189	Survey site	4 hrs	Mon 3/10/08	Mon 3/10/08		
190	General Installation - System, phones (including cut-off switches)	2 days	Mon 3/10/08	Wed 3/12/08	189	
191	**Test & Turn Up of Circuits on Site with LEC**	**0.5 days**	**Mon 3/10/08**	**Mon 3/10/08**		
192	Test & Turn Up Circuits	2 hrs	Mon 3/10/08	Mon 3/10/08		
193	Circuits Active/Ready	2 hrs	Mon 3/10/08	Mon 3/10/08	192	
194	**Cutover Tasks**	**2.5 days**	**Thu 3/13/08**	**Mon 3/17/08**		
195	**Cutover, Test & Quality Check (QC) Tasks**	**2.5 days**	**Thu 3/13/08**	**Mon 3/17/08**		
196	Verify all Features working properly	0.5 days	Thu 3/13/08	Thu 3/13/08		
197	Verify phones work, port assignments/call groups set	2 days	Thu 3/13/08	Fri 3/14/08		
198	QC Checklist & Test Calls Completed	0.5 days	Mon 3/17/08	Mon 3/17/08		
199	**Cut Sheet & QC Workbook Completed**	**0.25 days**	**Mon 3/17/08**	**Mon 3/17/08**		
200	Site Cutover to New System	0 days	Mon 3/17/08	Mon 3/17/08		

Project: Alaska DOC
Date: Tue 1/15/08

Critical — Progress — Summary — External Tasks
Critical Split — Milestone — Project Summary — External Milestone
Task — Slack — Rolled Up Critical — Deadline
Split — Slippage — Rolled Up Critical Split

ID	Task Name	Duration	Start	Finish	Predecessors	Resources
201	Distribute Cut Sheet to Logistics Planning	1 hr	Mon 3/17/08	Mon 3/17/08		
202	Site Cutover Complete - Ready for Training	0 days	Mon 3/17/08	Mon 3/17/08	201	
203	Workstation & Firewall (If Required)	2 hrs	Mon 3/17/08	Mon 3/17/08		
204	**Training - Palmer - 24 phones**	**1 day**	**Tue 3/18/08**	**Tue 3/18/08**		**TRAINING**
205	Perform Customer Training	1 day	Tue 3/18/08	Tue 3/18/08		
206	Complete Training Sign Off Including Heat Ticket	1 hr	Tue 3/18/08	Tue 3/18/08		
207						
208	**Install Activities - Point MacKenzie - 12 phones**	**3.5 days**	**Tue 3/18/08**	**Fri 3/21/08**		**Team 3 - 2 Techs**
209	**Receipt & General Install Tasks**	**1.5 days**	**Tue 3/18/08**	**Wed 3/19/08**		
210	Travel to site	0.5 days	Tue 3/18/08	Tue 3/18/08		
211	Receive System Shipment at Site	0 days	Tue 3/18/08	Tue 3/18/08	210	
212	Verify Shipment Content to Pick List	2 hrs	Tue 3/18/08	Tue 3/18/08		
213	Survey site	4 hrs	Tue 3/18/08	Tue 3/18/08		
214	General Installation - System, phones (including cut-off switches)	1 day	Tue 3/18/08	Wed 3/19/08	213	
215	**Test & Turn Up of Circuits on Site with LEC**	**0.5 days**	**Tue 3/18/08**	**Tue 3/18/08**		
216	Test & Turn Up Circuits	2 hrs	Tue 3/18/08	Tue 3/18/08		
217	Circuits Active/Ready	2 hrs	Tue 3/18/08	Tue 3/18/08	216	
218	**Cutover Tasks**	**1.5 days**	**Thu 3/20/08**	**Fri 3/21/08**		
219	**Cutover, Test & Quality Check (QC) Tasks**	**1.5 days**	**Thu 3/20/08**	**Fri 3/21/08**		
220	Verify all Features working properly	0.5 days	Thu 3/20/08	Thu 3/20/08		
221	Verify phones work, port assignments/call groups set	0.5 days	Thu 3/20/08	Thu 3/20/08		
222	QC Checklist & Test Calls Completed	0.5 days	Fri 3/21/08	Fri 3/21/08		
223	**Cut Sheet & QC Workbook Completed**	**0.25 days**	**Fri 3/21/08**	**Fri 3/21/08**		
224	Site Cutover to New System	0 days	Fri 3/21/08	Fri 3/21/08		
225	Distribute Cut Sheet to Logistics Planning	1 hr	Fri 3/21/08	Fri 3/21/08		
226	Site Cutover Complete - Ready for Training	0 days	Fri 3/21/08	Fri 3/21/08	225	
227	Workstation & Firewall (If Required)	2 hrs	Fri 3/21/08	Fri 3/21/08		
228	**Training - Point MacKenzie - 12 phones**	**1 day**	**Fri 3/21/08**	**Fri 3/21/08**		**TRAINING**
229	Perform Customer Training	1 day	Fri 3/21/08	Fri 3/21/08		
230	Complete Training Sign Off Including Heat Ticket	1 hr	Fri 3/21/08	Fri 3/21/08		
231						
232	**Install Activities - Spring Creek - 30 phones**	**4.5 days**	**Mon 3/24/08**	**Fri 3/28/08**		**Team 3 - 2 Techs**
233	**Receipt & General Install Tasks**	**2.5 days**	**Mon 3/24/08**	**Wed 3/26/08**		
234	Travel to site	0.5 days	Mon 3/24/08	Mon 3/24/08		
235	Receive System Shipment at Site	0 days	Mon 3/24/08	Mon 3/24/08	234	
236	Verify Shipment Content to Pick List	2 hrs	Mon 3/24/08	Mon 3/24/08		
237	Survey site	4 hrs	Mon 3/24/08	Mon 3/24/08		
238	General Installation - System, phones (including cut-off switches)	2 days	Mon 3/24/08	Wed 3/26/08	237	
239	**Test & Turn Up of Circuits on Site with LEC**	**0.5 days**	**Mon 3/24/08**	**Mon 3/24/08**		
240	Test & Turn Up Circuits	2 hrs	Mon 3/24/08	Mon 3/24/08		

Project: Alaska DOC
Date: Tue 1/15/08

Critical	Progress	Summary	External Tasks		
Critical Split	Milestone	Project Summary	External Milestone		
Task	Slack	Rolled Up Critical	Deadline		
Split	Slippage	Rolled Up Critical Split			

ID	Task Name	Duration	Start	Finish	Predecessors	Resources
241	Circuits Active/Ready	2 hrs	Mon 3/24/08	Mon 3/24/08	240	
242	**Cutover Tasks**	**1.5 days**	**Thu 3/27/08**	**Fri 3/28/08**		
243	**Cutover, Test & Quality Check (QC) Tasks**	**1.5 days**	**Thu 3/27/08**	**Fri 3/28/08**		
244	Verify all Features working properly	0.5 days	Thu 3/27/08	Thu 3/27/08		
245	Verify phones work, port assignments/call groups set	1 day	Thu 3/27/08	Thu 3/27/08		
246	QC Checklist & Test Calls Completed	0.5 days	Fri 3/28/08	Fri 3/28/08		
247	**Cut Sheet & QC Workbook Completed**	**0.25 days**	**Fri 3/28/08**	**Fri 3/28/08**		
248	Site Cutover to New System	0 days	Fri 3/28/08	Fri 3/28/08		
249	Distribute Cut Sheet to Logistics Planning	1 hr	Fri 3/28/08	Fri 3/28/08		
250	Site Cutover Complete - Ready for Training	0 days	Fri 3/28/08	Fri 3/28/08	249	
251	Workstation & Firewall (If Required)	2 hrs	Fri 3/28/08	Fri 3/28/08		
252	**Training - Spring Creek - 30 phones**	**1 day**	**Fri 3/28/08**	**Fri 3/28/08**		**TRAINING**
253	Perform Customer Training	1 day	Fri 3/28/08	Fri 3/28/08		
254	Complete Training Sign Off Including Heat Ticket	1 hr	Fri 3/28/08	Fri 3/28/08		
255						
256	**Install Activities - Wildwood - 35 phones**	**4.5 days**	**Mon 3/31/08**	**Fri 4/4/08**		**Team 2 - 2 Techs**
257	**Receipt & General Install Tasks**	**2.5 days**	**Mon 3/31/08**	**Wed 4/2/08**		
258	Travel to site	0.5 days	Mon 3/31/08	Mon 3/31/08		
259	Receive System Shipment at Site	0 days	Mon 3/31/08	Mon 3/31/08	258	
260	Verify Shipment Content to Pick List	2 hrs	Mon 3/31/08	Mon 3/31/08		
261	Survey site	4 hrs	Mon 3/31/08	Mon 3/31/08		
262	General Installation - System, phones (including cut-off switches)	2 days	Mon 3/31/08	Wed 4/2/08	261	
263	**Test & Turn Up of Circuits on Site with LEC**	**0.5 days**	**Mon 3/31/08**	**Mon 3/31/08**		
264	Test & Turn Up Circuits	2 hrs	Mon 3/31/08	Mon 3/31/08		
265	Circuits Active/Ready	2 hrs	Mon 3/31/08	Mon 3/31/08	264	
266	**Cutover Tasks**	**1.5 days**	**Thu 4/3/08**	**Fri 4/4/08**		
267	**Cutover, Test & Quality Check (QC) Tasks**	**1.5 days**	**Thu 4/3/08**	**Fri 4/4/08**		
268	Verify all Features working properly	0.5 days	Thu 4/3/08	Thu 4/3/08		
269	Verify phones work, port assignments/call groups set	1 day	Thu 4/3/08	Thu 4/3/08		
270	QC Checklist & Test Calls Completed	0.5 days	Fri 4/4/08	Fri 4/4/08		
271	**Cut Sheet & QC Workbook Completed**	**0.25 days**	**Fri 4/4/08**	**Fri 4/4/08**		
272	Site Cutover to New System	0 days	Fri 4/4/08	Fri 4/4/08		
273	Distribute Cut Sheet to Logistics Planning	1 hr	Fri 4/4/08	Fri 4/4/08		
274	Site Cutover Complete - Ready for Training	0 days	Fri 4/4/08	Fri 4/4/08	273	
275	Workstation & Firewall (If Required)	2 hrs	Fri 4/4/08	Fri 4/4/08		
276	**Training - Wildwood - 35 phones**	**1 day**	**Fri 4/4/08**	**Fri 4/4/08**		**TRAINING**
277	Perform Customer Training	1 day	Fri 4/4/08	Fri 4/4/08		
278	Complete Training Sign Off Including Heat Ticket	1 hr	Fri 4/4/08	Fri 4/4/08		
279						
280	**Install Activities - Yukon - 15 phones**	**3.5 days**	**Mon 3/31/08**	**Thu 4/3/08**		**Team 3 - 2 Techs**

Project: Alaska DOC
Date: Tue 1/15/08

Critical	Progress	Summary	External Tasks		
Critical Split	Milestone	Project Summary	External Milestone		
Task	Slack	Rolled Up Critical	Deadline		
Split	Slippage	Rolled Up Critical Split			

ID	Task Name	Duration	Start	Finish	Predecessors	Resources
281	**Receipt & General Install Tasks**	**1.5 days**	**Mon 3/31/08**	**Tue 4/1/08**		
282	Travel to site	0.5 days	Mon 3/31/08	Mon 3/31/08		
283	Receive System Shipment at Site	0 days	Mon 3/31/08	Mon 3/31/08	282	
284	Verify Shipment Content to Pick List	2 hrs	Mon 3/31/08	Mon 3/31/08		
285	Survey site	4 hrs	Mon 3/31/08	Mon 3/31/08		
286	General Installation - System, phones (including cut-off switches)	1 day	Mon 3/31/08	Tue 4/1/08	285	
287	**Test & Turn Up of Circuits on Site with LEC**	**0.5 days**	**Mon 3/31/08**	**Mon 3/31/08**		
288	Test & Turn Up Circuits	2 hrs	Mon 3/31/08	Mon 3/31/08		
289	Circuits Active/Ready	2 hrs	Mon 3/31/08	Mon 3/31/08	288	
290	**Cutover Tasks**	**1.5 days**	**Wed 4/2/08**	**Thu 4/3/08**		
291	**Cutover, Test & Quality Check (QC) Tasks**	**1.5 days**	**Wed 4/2/08**	**Thu 4/3/08**		
292	Verify all Features working properly	0.5 days	Wed 4/2/08	Wed 4/2/08		
293	Verify phones work, port assignments/call groups set	0.5 days	Wed 4/2/08	Wed 4/2/08		
294	QC Checklist & Test Calls Completed	0.5 days	Thu 4/3/08	Thu 4/3/08		
295	**Cut Sheet & QC Workbook Completed**	**0.25 days**	**Thu 4/3/08**	**Thu 4/3/08**		
296	Site Cutover to New System	0 days	Thu 4/3/08	Thu 4/3/08		
297	Distribute Cut Sheet to Logistics Planning	1 hr	Thu 4/3/08	Thu 4/3/08		
298	Site Cutover Complete - Ready for Training	0 days	Thu 4/3/08	Thu 4/3/08	297	
299	Workstation & Firewall (If Required)	2 hrs	Thu 4/3/08	Thu 4/3/08		
300	**Training - Yukon - 15 phones**	**1 day**	**Fri 4/4/08**	**Fri 4/4/08**		**TRAINING**
301	Perform Customer Training	1 day	Fri 4/4/08	Fri 4/4/08		
302	Complete Training Sign Off Including Heat Ticket	1 hr	Fri 4/4/08	Fri 4/4/08		

Project: Alaska DOC
Date: Tue 1/15/08

Critical
Critical Split
Task
Split
Progress
Milestone
Slack
Slippage
Summary
Project Summary
Rolled Up Critical
Rolled Up Critical Split
External Tasks
External Milestone
Deadline

Attachment I

SECURUS Test/Acceptance Plan

Installers Name: _____ **Date:** _____

Facility: _____

Yes/No/NA

1) Site i Inventory

a) Does the equipment received match the Sales Order? Yes

Notes: _____

b) Was all the equipment received without damage? Yes

Notes: _____

c) Is equipment received correct for the installation? Yes

Notes: _____

2) Equipment location and Security

a) Is there sufficient HVAC in the phone room? Yes

Notes: _____

b) Is there sufficient floor and wall space available? Yes

Notes: _____

c) Is the room in a secure location? Yes

Notes: _____

3) Power/Grounding

a) Is a grounded, dedicated circuit being used to power the equipment? No

Notes: _____

b) Is the platform and all related electronic equipment grounded w/ #12 green insulated copper wire? Yes

Notes: _____

4) UPS/Battery back up

a) Is all the Securus equipment on a UPS/Battery back up? Yes

Notes: _____

b) Is the UPS plugged into the Towermax KSU? Yes

Notes: _____

5) Lightning Protection

a) Is the Towermax KSU installed and electrically grounded? Yes

Notes:

b) Is there lightning protection installed on the C.O. side of the system? Yes

Notes:

c) Is there lightning protection installed on the station side of the system? No

(pertains to campus environments and areas that require ie., FL)

Notes:

6) Connectivity to Workstations

a) Are all the workstations installed and connected to the hub? Yes

Notes:

b) Are the all the monitors working? Yes

Notes:

c) Are all the printers installed and a test page printed? Yes

Notes:

d) Are the speakers installed and working? Yes

Notes:

e) Are the keyboards and mice installed and working? Yes

Notes:

7) Provisioning

a) Have all the lines/circuits been identified and terminated? Yes

Notes:

b) Have the lines been tested? Yes

Notes:

c) Local Dialing - 7 or 10 digit? Yes

Notes:

d) 1010XXX, LD? Yes

Notes:

e) 800, 888? Yes

Notes:

f) I Plus? Yes

Notes:

g) Has the modem line been installed and tested? Yes

Notes:

8) Networking

a) Can all the workstations be pinged from Dallas? Yes

Notes:

b) Have the IP addresses for routers and channel banks been set and are visible to the network? N/A

Notes:

c) Have the routers and channel banks been programmed and tested? N/A

Notes:

d) Are firewalls in place if facility network is utilized? N/A

Notes:

9) Inmate Phones

a) Have all the phones been installed and securely mounted? Yes

Notes:

b) Are all the conduit, pedestals, and backboards securely fastened? Yes

Notes:

c) Have all the phones been tested and port ID's located? Yes

Notes:

d) Have all the port assignments been set up in the IAD config? Yes

Notes:

e) Are the on-off times set? Yes

Notes:

10) Coin phones

a) Coin phones are installed and securely mounted? N/A

Notes:

b) Did you use the Raleigh office test call procedure? N/A

Notes:

c) Have the coin phones been programmed by the Raleigh office? N/A

Notes:

d) Have test calls been made? N/A

Notes:

e) Local? N/A

Notes:

f) LD? N/A

Notes:

g) Call completed using coin? N/A

Notes:

h) Call not completed to insure coin return? N/A

Notes:

11) Visitation Phones

a) Are all the visitation phones installed and securely mounted? Yes

Notes:

b) Have the visitation phones been connected to the IAD system and tested? Yes

Notes:

c) Have all the visitation port ID's been set up in a separate phone group? Yes

Notes:

d) Have the on-off times been set? N/A

Notes:

e) Are the visitation phones set up for monitoring and recording? Yes

Notes:

12) TDD phones

a) Are the TDD phones installed and securely mounted? N/A

Notes:

b) Has a TDD to TDD call been tested? N/A

Notes:

c) Has the TDD relay station number been programmed into the CAM and test call placed? (1-800-Relay-State Abbr) Example - 1-800-735-2972 (SC) N/A

Notes:

13) Cut-off switches

a) Are the switches installed on a separate block and labeled? Yes

Notes:

b) Have the switches been tested? Yes

Notes:

c) Are all the inmate phones capable of being turned off by the switches? Yes

Notes:

14) Features

a) Live call monitoring tested? Yes

Notes:

b) Covert Alert tested? Yes

Notes:

c) Call recording tested? Yes

Notes:

d) Number blocking tested? Yes

Notes:

e) Turning phones on/off through the system tested? Yes

Notes:

f) Report generator tested with ability to print report with correct date and time? Yes

Notes:

g) CD burner tested? Yes

Notes:

h) Password set up for facility and working? Yes

Notes:

i) Crime Tip tested? Yes

Notes:

j) PIN/PAN tested? Yes

Notes:

k) Stop on DTMF tested? Yes

Notes:

l) System Debit tested? N/A

Notes:

m) Prepaid calling cards tested? N/A

Notes:

n) Rate Quote tested and verified? N/A

Notes:

o) 3-Way detect tested? No

Notes:

p) All language options set? Yes

Notes:

q) Inmate Voice Mail tested? Yes

Notes:

15) Test Calls *Each system each station card*

a) Positive acceptance tested? Yes

Notes:

b) Tag line correct for the facility? Yes

Notes:

c) System prompts you for the recording of your name? Yes

Notes:

d) Both parties are prompted the call is subject to monitoring and recording? Yes

Notes:

e) Local collect tested with val Local rates verified to be correct? Yes

Notes:

f) Domestic LD collect tested ' Long Distance rates vefified to be correct? Yes

Notes:

g) Rates upon request tested? N/A

Notes:

h) Intrastate Debit (NPA-700-4141) tested? N/A

Notes:

i) Interstate Debit (700-555-4141) tested? N/A

Notes:

j) International LD Debit (011-458-0199-048 Denmark Operator) tested? N/A

Notes:

k) Global Speed dial numbers tested? Yes

Notes:

l) Calls placed using all language options? Yes

Notes:

m) Standard blocked number tested? Yes

Notes:

n) Harassment block tested? No

Notes:

o) Free call tested? Yes

Notes:

p) Private number tested? No

Notes:

q) Call time limit tested? Yes

Notes:

r) Is the inmate muted during acceptance of the call? Yes

Notes:

s) Does the system block additional digits from being dialed during the call process? Yes

Notes:

t) Test calls made using PIN number local, LD, International? Yes

Notes:

u) Test call made using PAN list? Yes

Notes:

16) Polling and Validation

a) Is validation turned on and functioning properly? Yes

Notes:

b) Has validation been tested with tech support? (list who you worked with) Yes

Notes:

c) Has the site been set up for nightly polling and tested with the NOC? Yes
(list who you confirmed this with)

Notes:

17) PIN/PAN site specific data

a) Previous blocked, free, watched, numbers are entered? Yes

Notes:

b) PIN numbers have been entered? Yes

Notes:

c) PAN numbers have been entered? Yes

Notes:

d) Daily time limit set and tested for all PIN accounts? N/A

Notes:

e) Debit amounts decrement according to contracted rate structure? N/A

Notes:

18) Block Labeling

a) Are all your blocks clearly labeled: Yes

Notes:

b) C.O. blocks? Yes

Notes:

c) Station blocks? Yes

Notes:

d) Cut-off switch blocks? Yes

Notes:

e) Do all the blocks have dust covers and are clearly Labeled "Securus"? Yes

Notes:

f) All cabling is neat and labeled? Yes

Notes:

19) EAR/Photos

a) Have you taken digital photos of all the IDF's and MDF's? Yes

Notes:

b) Have you filled out the EAR paperwork and left a copy onsite attached to the SCN system? Yes

Notes:

20) Training

a) Has the local field technician been notified of the install? Yes

Notes:

b) Have you given basic training on the system? Yes

Notes:

c) Manuals reviewed with the customer? Yes

Notes:

d) Has the Account Manager been notified to give formal training? Yes

Notes:

e) Has the customer been provided stick on labels contact names and telephone telephone contact names and telephone numbers? Yes

Notes:

Installer's Signature: _____

Date: _____

Attachment J

SECURUS Key Personnel Resumes

Ross F. Preston
3062 Hawks Glen
Tallahassee, FL 32312
(850) 907-8292

Qualifications Summary:

I have been in the telecommunication industry for over 24 years. During that time I have had increased responsibilities for sales and sales management with particular emphasis on delivery of complex managed services, IT solutions and network security. With a total of over 18 years with MCI, the past 11 years have been in a Government Marketing capacity with focus on needs analysis, sales and service of complex voice and data networking solutions.

2007 – Present

Securus Technologies
Account Executive
Department of Corrections
Position Responsibilities

- Establish relationships with Western State Secretaries/Directors
- Educate prospects on Secure Call Platform capabilities
- Manage existing Department of Corrections customer base
- Implement marketing strategy for prospects
- Prepare business case analysis for financial considerations
- Position new services utilizing existing connectivity

2000-2007

MCI/Verizon Business
Regional Sales Manager
Government and Education
Position Responsibilities:

- Develop opportunities for Government and Education within State of Florida
- Continue market penetration for existing contracts
- Establish new revenue generating products and services
- Manage 3,400 node Frame Relay State of Florida contract ($26M annually)
- Manage State of Florida 800, CentraNet and IT Hardware contracts ($13M annually)
- Supervise five Government Account Managers for Government and Education
- Position companies Next Generation Network solutions
- Manage Department of Corrections inmate telephone services ($20M+ annually)

1998-1999

Qwest Communications Inc.
Director of Sales
Position Responsibilities:

- Created marketing strategy for Southeast Region Business Markets Segment
- Devised plans for exceeding monthly, quarterly, and annual revenue attainment
- Established budgetary guidelines for all facets of the Southeast Region
- Supervised all Sales Managers in a four state area
- Developed forecasting tools for the management and sales teams
- Organized distribution of new pricing, products, and promotional materials
- Implemented account retention programs
- Oversaw completion of RFP and RFI responses
- Prepared business case analysis for financial committee review

1997-1998

MCI Telecommunications (Correctional Services Organization)
National Account Marketing Manager

Position Responsibilities:

- Managed inmate telecommunications service contracts ($43 Million annually)
- Influenced key decision markers to include MCI strengths in RFP (Nine States)
- Positioned enhanced services with existing contract bandwidth
- Developed partnerships with strategic vendors for reduction in COG
- Coordinated RFP responses with legal and business analysis

1994-1997 ***MCI Telecommunications (State Government and University Markets)***
National Account Marketing Manager

Position Responsibilities:

- Reviewed and analyzed sales and marketing plans for student resale programs
- Prepared revenue attainment forecasting by service offering
- Researched potential new products and services
- Supervised sales, support, and marketing representatives
- Initiated sales teaming efforts with BellSouth in LA
- Prepared RFP responses for State of Florida and Louisiana communication services
- Oversaw the Card Application Technology Center program with FSU

1987-1994 ***MCI Telecommunications (Business Markets)***
Sales Manager III

- Responsible for commercial sales for the Florida Panhandle
- Supervised sales teams in four city region
- Responsible for revenue attainment and forecasting
- Development of sales team product and industry knowledge
- Overall management of the commercial business customers and prospects

Education:

University of Florida (1978-1980)

HELEN L. MCCOY
429 W. Bear Lake Rd. N.E.
Kalkaska, MI 49646 U.S.A.
231-258-4971

STRENGTHS Customer focused. Highly motivated self-starter with excellent problem solving skills.

EXPERIENCE

T-NETIX/SECURUS

01-01 to Present **Implementation/Project Manager, Corrections**

- Coordinate & implement comprehensive call monitoring & recording system for inmate market throughout the U.S. and Canada.
- Successfully managed & implemented the following large scale projects recently:
    - Kentucky DOC – 16 facilities
    - South Carolina DOC – 32 facilities
    - Pennsylvania DOC – 6 facilities
    - Marion County Jail, IN – 5 facilities
- Currently engaged in the following implementation:
    - Florida DOC – 140 facilities – worth 20M annually
- Handle special projects as assigned, i.e., Verizon traffic conversion project, Iowa DOC conversion project, Hillsborough County Florida conversion project, long distance contract for INDOC along with "Called Party Pre-Paid", "Called Party Pre-Paid" for KSDOC, performed evaluation at New Jersey DOC to determine best course of action to resolve customer dissatisfaction with centralized IPIN process.
- Resolve service concerns/issues to ensure customer satisfaction.

SBC/AMERITECH

06-99 to 12-00 **Implementation/Project Manager, Pay Phone Services-Corrections**

- Coordinated & implemented comprehensive call monitoring & recording system for State of Michigan D.O.C. inmate phones (36 sites, prisons/camps), County/City jails (60 customers with various number of locations per customer) in Michigan & Grand Junction, Colorado.
- SME for Magnasync Solution as designed for State of Michigan, D.O.C.
- Instructor for all initial & continuation Magnasync training at customer sites.
- Resolved service concerns/issues to ensure customer satisfaction.
- Negotiated & hire contractors for work in non-Ameritech locations.

02-97 to 06-99 **Manager-Contract Compliance, CBS**

- Monitored & measured Managed Service contracts to ensure customer satisfaction & Ameritech profitability within the boundaries of the contract.
- Compiled & published metric performance results for assigned Managed Services accounts, NBD, American Axle, EDS, Ford, FOA, OfficeMax, and Kraft Video on a monthly and/or weekly basis. Use this data to compile quarterly, bi-annual, or annual performance results for respective customers.
- Analyzed performance results and offer recommendations for process or procedure improvements to enhance performance results.
- Actively participated on cross-functional teams/task forces in support of activities to optimize performance on Managed Service projects.

09-96 to 02-97 **Account Service Administrator, CBS**

- Coordinated & implemented complex services for Health Care accounts, Sister's of St. Joseph (St. John Hospital, Borgess Health Alliance, Genesys Health Systems) & Oakwood Health System.
- Resolved service & billing issues.
- Supported Account Executive by providing data via reports from within the Ameritech system or by generating customized reports.

01-95 to 09-96 **Project Manager, Pay Phone Services-Corrections**

- Coordinated & implemented comprehensive call monitoring & recording system for State of Michigan D.O.C. inmate phones (36 sites, prisons/camps).
- SME for Magnasync Solution as designed for State of Michigan, D.O.C.
- Instructor for all initial & continuation Magnasync training at customer sites.

HELEN L. MCCOY
429 W. Bear Lake Rd. N.E.
Kalkaska, MI 49646 U.S.A.
231-258-4971

1989-1995 **Manager-Administration, Operations & Database, Market Services**

- Directed & managed regional database for tracking sales projects.
- Directed, coordinated, & controlled special projects generated by external & internal customers.
- Developed, allocated & monitored district & manager level expense budgets ($7M annually).
- System administrator for NCR Tower & district PC LAN system.
- Special Events Coordinator for district, i.e., 2 day conference for 110 district employees, all day district meetings - off premise, etc.
- Provided administrative/procedural support to district employees (93 Mgmt & 17 N-Mgmt).
- Supervised seven front-line employees.
- Developed & implemented call handling procedures for front-line employees.
- Investigated, coordinated, & implemented new phone system for district.

1986-1989 **Sales & Service Clerical, Market Services**

- Received & answered inquires from internal & external customers.
- Negotiated & issued telephone service orders for external customers.
- Performed other clerical duties as necessary.
- Performed District Secretary function as needed.

1970-1986 **Held a Variety of Non-Management Positions**

- Residence Service Representative, Service Evaluator, Service Assistant, General Commercial Clerk, Operator.

Computer Skills: Proficient using Microsoft Windows XP, Word, Excel, Access, Project, Visio.

EDUCATION: Attended Washtenaw Community College.

Kenneth Rose

2118 Creek Ct.. Newman, CA 95360 209-862-2122

Current Position: Regional Operations Manager for Securus Technologies

HIGHLIGHTS OF QUALIFICATIONS

- 28 years in the Telecommunications Field, the last 11 years in Inmate Services
- Masters Degree in Computer Information Systems and a Bachelor Science in Business – Labor Relations.
- Considered an IT specialist with extensive experience in all aspects of telephony, PC-based hardware/software installation and configuration – primarily Inmate Calling Platforms
- Successfully manage over 300 Inmate Sites, with over 16,000 stations in Alaska, California, Hawaii, Oregon and Washington.
- Versatile, innovative, and diplomatic while maintaining a professional attitude
- Excellent Oral and Written Skills, Proactive in research, problem-resolution and Customer Service

RELEVANT SKILLS AND ACCOMPLISHMENTS

Administrative

- Currently supervise 14 technical staff members, including personnel evaluations and time reporting.
- Successfully managed various dispatch and contractor expenses utilizing the company's profit center guidelines.
- Continually work with associates and contractors to monitor and reduce our cost per line expense.
- Developed and Implemented a comprehensive Service Plan for the West Coast Region encompassing the states of AZ, AK, CA, HI, ID, NV, OR, & WA, including AK DOC & WA DOC Facilities
- Successfully developed, and had approved by Legal, a Contractor's agreement for all Field Service Contractors to sign in order to perform work for Securus.

Interpersonal/Teamwork

- Over 28 years in Customer service, primarily Inmate Accounts for the last 11 years
- Recognized on numerous occasions for Customer Service by various Customers and Partners
  - FSH, AT&T, SBC, Verizon and QWEST
- Successfully empowered associates to meet the needs of the business, while keeping the focus on Service.
- As Customer Service Manager for AT&T, responsible for portfolio of Accounts with a market value of $72 Million and project managing the end to end process in contract implementation.
- Consistently work to achieve the Company's Mission Statement, utilizing empowerment and cost savings to provide excellent quality customer service.
- Work closely with associates and the Sales Team in achieving all established goals and targets.

Technical Support

- Certified by the State of California to teach in all Collegiate and Secondary Education Facilities – CBEST certification.
- Certified in PQMI (Process Quality Management Improvement) – Metrics and implementation processes
- Certified as a Trained Facilitator by AT&T, provided training sessions over span of 6 years.
- Well versed in all aspects of Telephony, including PBX, Central Office, and 5ESS switching & routing.
- As the 5ESS Switch Administration of the ANHM & SHOK 5E's in Southern California, was responsible for processing 10% of all AT&T Operator assisted traffic handled in the United States
- Responsible for the successful installation and maintenance of over 18,000 phones and various call processing systems
- Fluent in all Microsoft Operating systems up to and including Windows 2000 & XP. In addition to various other Operation systems and programs, including but not limited to: pcAnywhere, UNIX, MS OFFICE Suites

EMPLOYMENT HISTORY

2001 to Date	**Securus Technologies – Field Operations** Irving, TX	*West Coast Regional Manager* *- Customer Support Manager*
1998 to 2001	**AT&T – Consumer Services** Pleasanton, CA	*Customer Service Manager* *– Inmate Markets*
1989 to 1998	**AT&T – Network Services** Pleasanton, CA	*5ESS Switch Administrator,* *- Screening Administrator*
1979 to 1989	**AT&T – Operator Services** Santa Clara, CA	*Rates & Tariff Associate,* *- Operator Services Associate*

EDUCATION HISTORY

1998	University of Phoenix	Master's Degree – MSCIS
1992	University of Phoenix	Bachelor's Science Degree – BSBA/Labor Relations

JAMES G. LEBOEUF – PRODUCT ENGINEER

Summary of Qualifications

James has supported inmate systems and correctional facility accounts for over 17 years in Operations Management and Technical Sales. He has been directly involved with Installation and Maintenance of 300+ correctional facilities and indirectly involved as team management for 1000+ facilities throughout the Continental US and Alaska.

Experience

1989–present SECURUS Technologies Irving, TX

Technical Sales Support Manager

Support technical solutions development within Evercom

Ensure the highest quality delivery of Partner projects

Support product/feature development process

Provide "Best in Class" internal/external customer support

Consult with customers, identify technical requirements, present viable solutions and drive flawless execution of the agreed solution.

(Acquired by Evercom) Peoples TELINK Bryan, TX

Field Service Manager

Oversee Field Maintenance Support of Law Enforcement Technologies for the Central Region

Hire and Train Field Service technicians

Responsible for implementing and maintaining technical standards, assuring customer satisfaction

Engineer and implement WAN installation projects

Responsible for scheduling staff, delegating assignments and deadlines, conducting annual performance appraisals, and making salary increase recommendations

Identify Training Development Needs and conduct classes insuring next level development for all Regional Field technicians.

1981–1989 Cameron Telephone Company Carlyss, LA

Line Analyst

Analyze and recommend proactive maintenance for Business and Residential Telephone Customers

Serve as Technical Support for installation and repair technicians in a LEC environment

Train personnel on the installation and maintenance of Business Telephone Systems

Responsible for implementing remote test procedures of all Central Office Equipment including attached Outside Plant facilities

JASEN A. KINTNER
Anchorage, Alaska

SUMMARY OF QUALIFICATIONS

Sixteen years' combined telecommunications experience with the United States Army, General Communications, Inc., Communications Consultants, Inc., and Securus Technologies, Inc. Four-time Army medal awardee for outstanding job performance. Developed a course of instruction for a company of 185 people which resulted in improved and enhanced communications in fixed, mobile, and remote site locations. Adapts readily to difficult situations and works hard to produce a favorable solution. Loyal, disciplined, and very detail-oriented.

TELECOMMUNICATIONS

Installed, initialized, operated, and performed maintenance on digital telecommunications switching systems. Analyzed and identified call processing trouble. Used Lucent 5ESS-2000 Trunk and Line Workstation to resolve maintenance problems. Built, loaded, and modified local databases to suit operational needs. Responded to maintenance triggers for line or trunk failures. Interpreted computer printouts to troubleshoot, repair, or replace faulty line units. Coordinated with system operators and managers to resolve communications difficulties. Troubleshot complex system faults and supervised or corrected failures to meet system availability and reliability standards. Recorded number of daily communications transactions and number of problems to include actions taken to correct the problem, using a computer workstation. Acquainted with all color codes for 100 pair cable. Installed cross connect wires on the main distribution frame. Terminated telephone cables to 410 type blocks. Fabricated and installed various communications and electrical cable and wire. Utilized special tools, wire wrap guns, and hand tools to connect cable and wire.

- Successfully connected U.S. Army and French Army communications equipment using NATO analog interface system.
- Provided reliable communications to over 1,000 subscribers with less than 5% down time while simulating a war-time environment.
- Helped develop and initialization standard for Node Center Switches of a 185 person communications unit.

MANAGEMENT

Organized and lead several 406 member teams to include Advanced Party Team, Nuclear Biological Chemical Team, and Field Sanitation Team. Initiated system to track the physical conditioning of 49 personnel. Established three unit college classes for 25 personnel. Oversaw the maintenance and accountability of three 1 ¼ ton heavy variant 4x4 vehicles equipped with shelter carriers and two 10 kilowatt generators. Designed maintenance checklist to track and improve vehicle readiness.

- Organized and directed large convoys of over 50 vehicles for a major military exercise during September 1997.
- Helped design signal-site layout plans for a 50-person communications platoon which resulted in improved site defense and faster, more efficient installation time.

JASEN A. KINTNER

COMPUTER

Used computers to perform system and network operations ranging from initialization and installation to troubleshooting. Ensured that systems were operated and maintained according to Army regulations. Verified that users had the required personal security clearances, authorizations, and need-to-know. Provided semiannual training to users, operators, and managers. Familiar with basic UNIX commands. Knowledgeable of several operating systems to include Windows 95, 98, NT 4.0, 2000 and XP. Proficient with various software applications and programming languages.

- Developed and documented an updated standard for registering computer users from Node Center Switch which resulted in enhanced X.25 networking using Windows 95 and Windows 4.0.
- Improved maintenance management posture for nine workstations in a communications unit; achieved minimal downtime over a three year period.

ELECTRICAL

Assisted electrician in installation and placement of conduit and electrical wiring. Measured and cut pipe conduit to specified length. Drilled holes for wiring and pulled or pushed wiring through opening. Traced out short circuit in wiring, using knowledge of wiring and test meter. Performed minor repairs; replaced fuses, light sockets, bulbs, and switches. Disassembled defective electrical equipment, replaced defective or worn parts, and reassembled equipment. Maintained tools and equipment, and kept supplies and parts in order.

RELATED EXPERIENCE

Field Service Technician II, Securus Technologies, Inc., Anchorage, Alaska 2002-Present
President, Gallant Technologies, Inc., Anchorage, Alaska 2000-2002
Testboard Technician, Communications Consultants, Inc., Anchorage, Alaska 1999
Switch Technician II, General Communications, Inc., Anchorage, Alaska 1998-1999
Central Office Frame Wirer, Infotel International, Inc., Anchorage, Alaska 1997-1998
Information Systems Security Administrator, U.S. Army, Fort Richardson, Alaska 1996-1998
Network Switching Systems Technician, U.S. Army, Fort Richardson, Alaska 1991-1998
Electrician Helper, Freddie E. Norris Electrical Contractor, Inc., Evans, Georgia 1991

EDUCATION & CERTIFICATIONS

- Continuing College Education, University of Alaska Anchorage 2006 (84 Credit Hours)
- CompTIA A+ Certification, Anchorage, AK, 1998
- Diploma, Evans High School, Evans, Georgia 1991

MILITARY TRAINING

Primary Leadership Development Course, U.S. Army Fort Richardson, Alaska 1995
Leadership Development Course, U.S. Army, Darmstadt, Germany 1993 (**Honor Graduate**)
Digital Networking Systems Course, U.S. Army, Fort Gordon, Georgia 1991

KEVIN COLLINS

National Account Manager/Senior Account Executive
P.O. Box 4223
Greenwood Village, CO 80155-4223

Ph: 720-488.5696
Fax: 972-277-0651
kcollins3@securustech.net
Years with SECURUS: 12

EDUCATIONAL BACKGROUND:

BA Interdivisional Majors

History/English

Political Science/ Communications

Regis University, Denver, Colorado

PROFESSIONAL QUALIFICATIONS:

- 23 Years Experience in Telecommunications
- 12 Years Experience in Inmate Call Control Systems
- Extensive Experience in all aspects of Telephony
- More than 11 years with Bell System
- Over 23 years experience in telecommunications in complex solutions/implementations
- While with the Bell System, successfully maintained an Account base worth in excess of $100 Million per year in revenue

CURRENT RESPONSIBILITIES:

- National Account Manager serving the State Department of Corrections market and Canadian Correctional Market
- Primary Account Manager for selected DOC sites
- Manage the DOC account responsibilities with service and operational personnel.
- Maintain and execute customer scheduled briefings that include the following initiatives:
  - Site reviews with service team,
  - Offering product enhancements,
  - Identifying operational issues and offering solutions with various applications
- Updating customers on new introductions of applications and technology

Resume

Andrew L Fall

Andy Fall is the current Account Manager for Securus Technologies serving the Alaska DOC and has acted in that capacity since December 2004. Andy currently provides Account Management for facilities in Idaho, Oregon and Washington as well.

Andy has over 10 years experience in sales and sales support of Inmate Telephone Systems to City, County, State and Special Jurisdictions and over 20 years experience in sales and sales support of products and services to the Corrections Industry including commissary, trust fund software and identification biometrics.

Andy holds an undergraduate degree from Whittier College and a graduate degree from Pepperdine University.

Andy is based in Portland, Oregon.

Attachment K

SECURUS MSA and Service Schedule

SECURUS™ TECHNOLOGIES

Master Services Agreement
(_____)

This Master Services Agreement (this "Agreement") is by and between _____ ____ ("Customer") and Evercom Systems, Inc. [redacted] a Delaware corporation and a SECURUS Technologies, Inc. company, ("we," "us," or "Provider"). This Agreement shall be effective as of the date signed by Customer provided the agreement is received by Provider within ten (10) days thereof (the "Effective Date").

1. Applications. This Agreement specifies the general terms and conditions under which we will perform certain inmate-related services and applications (the "Application(s)") for you. Additional terms and conditions with respect to the Applications will be specified in the schedules entered into by the parties and attached hereto (the "Schedules"). The Schedules are incorporated into this Agreement and are subject to the terms and conditions of this Agreement. In the event of any conflict between this Agreement and a Schedule, the terms of the Schedule shall govern. In the event of any conflict between any two Schedules for a particular Application, the latest in time shall govern.

2. Use of Applications. You grant us the right and license to install, maintain, and derive revenue from the Applications through our inmate systems (including, without limitation, the related hardware and software) (the "System") located in and around the inmate confinement facilities identified on the Schedules (the "Facilities"). You are responsible for the manner in which you use the Applications. Unless expressly permitted by a Schedule or separate written agreement with us, you will not resell the Applications or provide access to the Applications (other than as expressly provided in a particular Schedule), directly or indirectly, to third parties. During the term of this Agreement and subject to the remaining terms and conditions of this Agreement, Provider shall be the sole and exclusive provider of inmate related communications, including but not limited to voice, video and data (phone calls, video calls, messaging, and e-mail) at the Facilities in lieu of any other third party providing such inmate communications, including without limitation, Customer's employees, agents or subcontractors.

3. Compensation. Compensation for each Application, if any, and the applicable payment addresses are as stated in the Schedules.

4. Term.

The obligations of the parties under this Agreement are effective as of the Effective Date but the "Term" of this Agreement shall commence sixty (60) days thereafter [to allow for a reasonable installation period] and will continue for __ years thereafter.

[redacted] Notwithstanding anything to the contrary, the terms and conditions of this Agreement shall continue to apply to each Schedule for so long as we continue to provide the Application to you after the expiration or earlier termination of this Agreement.

5. Service Level Agreement and Limited Remedy. We are committed to providing you with reliable, high quality Applications, and we offer certain assurances about the quality of our Applications (the "Service Level Agreement"). The Service Level Agreement for each Application is as set forth in the applicable Schedule. THE SERVICE LEVEL AGREEMENT IS THE SOLE AND EXCLUSIVE REMEDY FOR FAILURE OR DEFECT OF AN APPLICATION. WE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM A COURSE OF DEALING OR USAGE OF TRADE, AND NONINFRINGEMENT.

6. Software License. We grant you a personal, non-exclusive, non-transferable license (without the right to sublicense) to access and use certain proprietary computer software products and materials in connection with the Applications (the "Software"). The Software includes any upgrades, modifications, updates, and additions to existing features that we implement in our discretion (the "Updates"). Updates do not include additional features and significant enhancements to existing features. Your rights to use any third-party software product that we provide shall be limited by the terms of the underlying license that we obtained for such product. The Software is to be used solely for your internal business purposes in connection with the Applications at the Facilities. You will not (i) permit any parent, subsidiary, affiliated entity, or third party to use the Software, (ii) assign, sublicense, lease, encumber, or otherwise transfer or attempt to transfer the Software or any portion thereof, (iii) process or permit to be processed any data of any other party with the Software, (iv) alter, maintain, enhance, disassemble, decompile, reverse engineer or otherwise modify the Software or allow any third party to do so, (v) connect the Software to any products that we did not furnish or approve in writing, or (vi) ship, transfer, or export the Software into any country, or use the Software in any manner prohibited by the export laws of the United States. We are not liable with regard to any Software that you use in a prohibited manner.

7. Ownership and Use. The System, the Applications, and related records, data, and information shall at all times remain our sole and exclusive property unless prohibited by law, in which event, we shall have the unlimited right to use such records, data, and information for investigative and law enforcement purposes. However, during the term of this Agreement and for a reasonable period of time thereafter, we will provide you with reasonable access to the records. We (or our

licensors, if any) have and will retain all right, title, interest, and ownership in and to (i) the Software and any copies, custom versions, modifications, or updates of the Software, (ii) all related documentation, and (iii) any trade secrets, know-how, methodologies, and processes related to our Applications, the System, and our other products and services (the "Materials"). The Materials constitute proprietary information and trade secrets of Provider and its licensors, whether or not any portion thereof is or may be the subject of a valid copyright or patent.

8. Legality/Limited License Agreement. For services related to Applications which may allow you to monitor and record inmate or other administrative telephone calls, or transmit or receive inmate electronic messages ("e-mail"); by providing the Application, we make no representation or warranty as to the legality of recording or monitoring inmate or administrative telephone calls or transmitting or receiving inmate e-mail messages. Further, you retain custody and ownership of all recordings, and inmate e-mail messages; however you grant us a perpetual limited license to compile, store, and access recordings or inmate calls and access inmate e-mail messages for purposes of (i) complying with the requests of officials at the Facility, (ii) disclosing information to requesting law enforcement and correctional officials as they may require for investigative, penological or public safety purposes, (iii) performing billing and collection functions, or (iv) maintaining equipment and quality control purposes. This license does not apply to recordings of inmate calls or e-mail messages with their attorneys or to recordings or e-mail messages protected from disclosure by other applicable privileges.

9. Confidentiality. The System, Applications, and related call records and information (the "Confidential Information") shall at all times remain confidential to Provider. You agree that you will not disclose such Confidential Information to any third party without our prior written consent. Because you will be able to access confidential information of third parties that is protected by certain federal and state privacy laws through the Software and Applications, you shall only access the Software with computer systems that have effective firewall and anti-virus protection.

10. Indemnification. To the fullest extent allowed by applicable law but subject to the limitations in this Agreement, each party (the "Indemnifying Party") will, and does hereby agree to, defend, indemnify and hold harmless the other party (the "Indemnified Party") from and against any loss, cost, claim, liability, damage, and expense (including, without limitation, reasonable attorney's fees and expenses) brought or claimed by third parties or by the Indemnified Party (collectively, "Claims") arising out of (i) a breach of either party's representations, warranties and/or covenants contained herein or (ii) the gross negligence or willful misconduct of, or intellectual property infringement or alleged intellectual property infringement by, the Indemnifying Party and/or its employees, agents, or contractors in the performance of this Agreement. The Indemnified Party shall notify the Indemnifying Party promptly in writing of any Claims for which the Indemnified Party alleges that the Indemnifying Party is responsible under this section and the Indemnifying Party shall hereupon tender the defense of such Claims to the Indemnifying Party. The Indemnified Party shall cooperate in every reasonable manner with the defense or settlement of such Claims at the Indemnifying Party's expense. The Indemnifying Party shall not be liable under this section for settlements of Claims finalized solely by the Indemnified Party unless the Indemnifying Party has approved such settlement in advance or unless the defense of such Claims has been tendered to the Indemnifying Party in writing and the Indemnifying Party has failed to promptly undertake the defense.

11. Insurance. We maintain comprehensive general liability insurance having limits of not less than $2,000,000.00 in the aggregate. You agree to provide us with reasonable and timely written notice of any claim, demand, or cause of action made or brought against you arising out of or related to the utilization of the Applications and the System. We have the right to defend any such claim, demand, or cause of action at our sole cost and expense and within our sole and exclusive discretion. You agree not to compromise or settle any claim or cause of action arising out of or related to the utilization of the Applications or System without our prior written consent, and you are required to assist us with our defense of any such claim, demand, or cause of action.

12. Default and Termination. If either party defaults in the performance of any obligation under this Agreement, then the non-defaulting party shall give the defaulting party written notice of its default setting forth with specificity the nature of the default. If the defaulting party fails to cure its default within thirty (30) days after receipt of the notice of default, then the non-defaulting party shall have the right to terminate this Agreement upon thirty (30) days written notice and pursue all other remedies available to the non-defaulting party, either at law or in equity. Notwithstanding the foregoing, the thirty (30) day cure period shall be extended to ninety (90) days if the default is not reasonably susceptible to cure within such thirty (30) day period, but only if the defaulting party has begun to cure the default during the thirty (30) day period and diligently pursues the cure of such default. Notwithstanding the foregoing, if you breach your obligations in the section entitled "Software License" or the section entitled "Confidentiality", then we shall have the right to terminate this Agreement immediately.

13. Limitation of Liability. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, NEITHER PARTY SHALL HAVE ANY LIABILITY FOR INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES, LOSS OF PROFITS OR INCOME, LOST OR CORRUPTED DATA, OR LOSS OF USE OR OTHER BENEFITS, HOWSOEVER CAUSED AND EVEN IF DUE TO THE PARTY'S NEGLIGENCE, BREACH OF CONTRACT, OR OTHER FAULT, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR AGGREGATE LIABILITY TO YOU RELATING TO OR ARISING OUT OF THIS AGREEMENT, WHETHER IN CONTRACT, TORT OR OTHERWISE, SHALL NOT EXCEED THE AMOUNT WE PAID YOU DURING THE TWELVE (12) MONTH PERIOD PRIOR TO THE DATE THE CLAIM AROSE.

14. Uncontrollable Circumstance. We reserve the right to renegotiate or terminate this Agreement upon sixty (60) days advance written notice if circumstances other than those under our control related to the Facilities (including, without limitation, changes in rates, regulations, or operations mandated by law; material reduction in inmate population or capacity; material changes in jail policy or economic conditions; acts of God; actions you take for security reasons (such as lock-

downs)) negatively impact our business; however, we shall not unreasonably exercise such right. Further, Customer acknowledges that Provider's provision of the services is subject to certain federal, state or local regulatory requirements and restrictions which are subject to change from time-to-time and nothing contained herein to the contrary shall restrict Provider from taking any steps necessary to perform in compliance therewith.

15. Injunctive Relief. Both parties agree that a breach of any of the obligations set forth in the sections entitled "Software License," "Ownership and Use," and "Confidentiality" would irreparably damage and create undue hardships for the other party. Therefore, the non-breaching party shall be entitled to immediate court ordered injunctive relief to stop any apparent breach of such sections, such remedy being in addition to any other remedies available to such non-breaching party.

16. Force Majeure. Either party may be excused from performance under this Agreement to the extent that performance is prevented by any act of God, war, civil disturbance, terrorism, strikes, supply or market, failure of a third party's performance, failure, fluctuation or non-availability of electrical power, heat, light, air conditioning or telecommunications equipment, other equipment failure or similar event beyond its reasonable control; provided, however that the affected party shall use reasonable efforts to remove such causes of non-performance.

17. Notices. Any notice or demand made by either party under the terms of this Agreement or under any statute shall be in writing and shall be given by personal delivery; registered or certified U.S. mail, postage prepaid; or commercial courier delivery service, to the address below the party's signature below, or to such other address as a party may designate by written notice in compliance with this section. Notices shall be deemed delivered as follows: personal delivery – upon receipt; U.S. mail – five days after deposit; and courier – when delivered as shown by courier records.

18. Miscellaneous. This Agreement shall be governed by and construed in accordance with the laws of the State of Texas. No waiver by either party of any event of default under this Agreement shall operate as a waiver of any subsequent default under the terms of this Agreement. If any provision of this Agreement is held to be invalid or unenforceable, the validity or enforceability of the other provisions shall remain unaffected. This Agreement shall be binding upon and inure to the benefit of Provider and Customer and their respective successors and permitted assigns. Except for assignments to our affiliates or to any entity that succeeds to our business in connection with a merger or acquisition, neither party may assign this Agreement without the prior written consent of the other party. Each signatory to this Agreement warrants and represents that he or she has the unrestricted right and requisite authority to enter into and execute this Agreement, to bind his or her respective party, and to authorize the installation and operation of the System. Provider and Customer each shall comply, at its own expense, with all applicable laws and regulations in the performance of their respective obligations under this Agreement and otherwise in their operations. Nothing in this Agreement shall be deemed or construed by the parties or any other entity to create an agency, partnership, or joint venture between Customer and Provider. This Agreement cannot be modified orally and can only be modified by a written instrument signed by all parties. The parties' rights and obligations, which by their nature would extend beyond the termination, cancellation, or expiration of this Agreement, shall survive such termination, cancellation, or expiration (including, without limitation, any payment obligations for services or equipment received prior to such termination, cancellation, or expiration). This Agreement may be executed in counterparts, each of which shall be fully effective as an original, and all of which together shall constitute one and the same instrument. This Agreement, together with the exhibits and Schedules, constitutes the entire agreement of the parties regarding the subject matter set forth herein and supersedes any prior or contemporaneous oral or written agreements regarding the subject matter set forth herein.

EXECUTED as of the Effective Date.

CUSTOMER:	PROVIDER:
_____	Evercom Systems, Inc. T-NETIX, Inc.
By: _____	By: _____
Name: _____	Name: John J. Viola
Title: _____	Title: Vice President and General Manager
Date: _____	Date: _____
Customer's Notice Address:	Provider's Notice Address:
_____	14651 Dallas Parkway, Suite 600 Dallas, Texas 75254 Attention: General Counsel
	Provider's Payment Address:
	14651 Dallas Parkway, Suite 600 Dallas, Texas 75254 Attention: Accounts Receivable

SECURUS™ TECHNOLOGIES

Schedule
(_____)

This Schedule is between [Evercom Systems, Inc.] [T-NETIX, Inc.], a Delaware corporation and a SECURUS Technologies, Inc. company ("we" or "Provider"), and _____ ("you" or "Customer") and is part of and governed by the Master Services Agreement (the "Agreement") executed by the parties. The terms and conditions of the Agreement are incorporated herein by reference. This Schedule shall be coterminous with the Agreement ("Schedule Effective Date").

A. Applications. We will provide the following Applications:

CALL MANAGEMENT SERVICE

DESCRIPTION:

Secure Call Platform: Secure Call Platform ("SCP") provides, through its centralized net centric, VOIP, digital transmitted system, automatic placement of calls by inmates without the need for conventional live operator services. In addition, SCP provides the capability to (a) monitor and record inmate calls, (b) mark certain numbers as private to disable the monitoring and recording function, (c) automatically limit the duration of each call to a certain period designated by us, (d) maintain call detail records in accordance with our standard practices, (e) automatically shut the System on or off, and (f) allow free calls to the extent required by applicable law. We will be responsible for all billing and collections of inmate calling charges but may contract with third parties to perform such functions. SCP will be provided at the Facilities specified in the chart below.

COMPENSATION:

Collect Calls. We will pay you commission (the "Commission") in the amount of the applicable Collect Commission Percentage (as specified in the chart below) of the applicable revenue base (as specified in the chart below) that we earn through the completion of collect calls placed from the Facilities. "Gross Revenue" means all charges billed by us relating to collect calls placed from the Facilities. Gross Revenue may be verified by the detailed call records maintained by us, without any deduction or credit for bad debt or for billed calls that for any reason are not collected. Regulatory required and other items such as federal, state and local charges and taxes and fees are excluded. "Gross Billed and Collected Revenue" means all charges billed and collected by us relating to collect calls placed from the Facilities. Regulatory required and other items such as federal, state and local charges and taxes and fees are excluded. "Net Revenue" means all charges billed and collected by us relating to collect calls placed from the Facilities, less all local and long distance charges, billing and validation costs, and a reserve for bad debt. Regulatory required and other items such as federal, state and local charges and taxes and fees are excluded. We shall remit the Commission for a calendar month to you on or before the 30th day after the end of the calendar month in which the calls where made (the "Payment Date"). All Commission payments shall be final and binding upon you unless we receive written objection within sixty (60) days after the Payment Date. Your payment address is as set forth in the signature block below. You shall notify us in writing at least sixty (60) days prior to a Payment Date of any change in your payment address.

FACILITIES AND RELATED SPECIFICATIONS:

Facility Name and Address	Type of Call Management Service	Collect Commission Percentage	Revenue Base for Calculation of Commission	Payment Address

CENTRALIZED NET CENTRIC, VOIP, DIGITAL TRANSMITTED CALL MANAGEMENT SYSTEM

SERVICE LEVEL AGREEMENT

We agree to repair and maintain the System (inclusive of the SECUREworkstation defined below) in good operating condition (ordinary wear and tear excepted), including, without limitation, furnishing all parts and labor. All such maintenance shall be conducted in accordance with the service levels in Items 1 through 10 below. All such maintenance shall be provided at our sole cost and expense unless necessitated by any misuse of, or destruction, damage, or vandalism to any premises equipment by you (not inmates at the Facilities), in which case, we may recoup the cost of such repair and maintenance through either a Commission deduction or direct invoicing, at our option. You agree to promptly notify us in writing after discovering any misuse of, or destruction, damage, or vandalism to, the said equipment. If any portion of the System is interfaced with other devices or software owned or used by you or a third party, then we shall have no obligation to repair or maintain such other devices or software. This SERVICE LEVEL AGREEMENT does not apply to any provided *Open*workstation(s) (see below). For the services contemplated hereunder, we may provide, based upon the facilities requirements, two types of workstations (personal computer/desktop/laptop/terminal): (i) The "SECUREworkstation" is designed to satisfy facilities that require a secure direct link and full technical support of the Applications. Utilizing the Windows XP operating system, the SECUREworkstation is subject to full technical and field support services described herein, access to all applicable Applications and restricted user rights for facility personnel. No other third party software

may be installed on the SECUREworkstation; and (ii) The "*Open*workstation" is an open non-secured workstation which permits administrative user rights for facility personnel and allows the facilities an ability to add additional third party software. Ownership of the *Open*workstation is transferred to the facility along with a three-year product support plan with the hardware provider. We have no obligation to provide any technical and field support services for an *Open*workstation. CUSTOMER IS SOLELY RESPONSIBLE FOR THE MAINTENANCE OF ANY *OPEN*WORKSTATION(S)."

1. Outage Report; Technical Support. If either of the following occurs: (a) you experience a System outage or malfunction or (b) the System requires maintenance (each a "System Event"), then you will promptly report the System Event to our Technical Support Department ("Technical Support"). You may contact Technical Support 24 hours a day, seven days a week (except in the event of planned or emergency outages) by telephone at 866-558-2323, by email at TechnicalSupport@Evercom.net, or by facsimile at 800-368-3168. We will provide you commercially reasonable notice, when practical, prior to any Technical Support outage. For your calls to Technical Support, the average monthly call answer time is generally 120 seconds or less, provided however, that we will endeavor (but will not be obligated) to achieve an average monthly call answer time of 30 seconds.

2. Priority Classifications. Upon receipt of your report of a System Event, Technical Support will classify the System Event as one of the following four priority levels:

"Priority 1"	60% or more of the functionality of the System is adversely affected by the System Event
"Priority 2"	30%-59% of the functionality of the System is adversely affected by the System Event
"Priority 3"	5%-29% of the functionality of the System is adversely affected by the System Event
"Priority 4"	Less than 5% of the functionality of the System is adversely affected by the System Event

3. Response Times. After receipt notice of the System Event, we will respond to the System Event within the following time periods with a 95% or greater rate of accuracy:

Priority 1	4 hours
Priority 2	12 hours
Priority 3	24 hours
Priority 4	36 hours

4. Response Process. In the event of a System Event, where the equipment is located on Customer premises, Technical Support will either initiate remote diagnosis and correction of the System Event or dispatch a field technician to the Facility (in which case the applicable regional dispatcher will contact you with the technician's estimated time of arrival), as necessary. In the event of a System Event occurs in the centralized SCP system, technical support will initiate remote diagnosis and correction of the System Event.

5. Performance of Service. All of our repair and maintenance of the System will be done in a good and workmanlike manner at no cost to you except as may be otherwise set forth in the Agreement. Any requested modification or upgrade to the System that is agreed upon by you and us may be subject to a charge as set forth in the Agreement and will be implemented within the time period agreed by the parties.

6. Escalation Contacts. Your account will be monitored by the applicable Territory Manager and Regional Service Manager. In addition, you may use the following escalation list if our response time exceeds 36 hours: first to the Technical Support Manager or Regional Service Manager, as applicable, then to the Director of Field Services, then to the Executive Director, Service.

7. Notice of Resolution. After receiving internal notification that a Priority 1 System Event has been resolved, a member of our management team will contact you to confirm resolution. For a Priority 2 or 3 System Event, a member of our customer satisfaction team will confirm resolution.

8. Monitoring. We will monitor our back office and validation systems 24 hours a day, seven days a week.

9. Required IGR. You are responsible for providing a dedicated isolated grounded receptacle ("IGR") for use in connection with the primary System. Upon request we will provide you with the specifications for the IGR. If you are unable to or do not provide the IGR, then we will provide the IGR on a time and materials basis at the installer's then-current billing rates, provided that we are not responsible for any delay caused by your failure to provide the IGR.

10. End-User Billing Services and Customer Care. Our Correctional Billing Services division will maintain dedicated customer service representatives to handle end-user issues such as call blocking or unblocking and setting up end-user payment accounts. The customer service representatives will be available during reasonable business hours Monday through Saturday by telephone at 800-844-6591, by email at Support@CorrectionalBillingServices.com, and by facsimile at 800-578-2627. In addition, we will maintain an automated inquiry system on a toll-free customer service phone line that will

be available to end-users 24 hours a day, 7 days a week to provide basic information and handle most routine activities. We will also accept payments from end-users by credit card, check, and cash deposit (such as by money order or Western Union transfer).

Exhibit A: Customer Statement of Work

(___)

This Customer Statement of Work is made part hereto and governed by the Master Services Agreement (the "Agreement") executed between [Evercom Systems, Inc.] [T-NETIX, Inc.], a Delaware corporation and a SECURUS Technologies, Inc. company ("we" or "Provider"), and _____ ("you" or "Customer"). The terms and conditions of said Agreement are incorporated herein by reference. This Customer Statement of Work shall be coterminous with the Agreement.

A. Applications. The parties agree that the Applications listed in the Service Schedule shall be provided and in accordance with the Service Level Agreements as described in the applicable section of the Service Schedule to the Agreement.

B. Equipment. We will provide the following equipment in connection with the Applications:

C. Installation. Installation guidelines are as follows:

UNLESS OTHERWISE EXPRESSLY SET FORTH IN WRITING IN THIS SCHEDULE, NO APPLICATIONS, EQUIPMENT, INSTALLATION AND SPECIAL REQUIREMENTS OTHER THAN THOSE STATED ABOVE WILL BE PROVIDED; NO ORAL AGREEMENTS OR STATEMENTS ARE BINDING.

EXECUTED as of the Schedule Effective Date.

CUSTOMER:	PROVIDER:
_____	Evercom Systems, Inc.
	T-NETIX, Inc.
By: _____	By: _____
Name: _____	Name: John J. Viola
Title: _____	Title: Vice President and General Manager

Attachment L

Signed Amendments

Attachment 2

RFP RECEIPT ACKNOWLEDGMENT FORM

(Return to Procurement Officer listed on page 1 as soon as possible)

INMATE TELEPHONE SYSTEM

RFP # 2008-2000-7549

ISSUED

December 19, 2007

I have received the above specified RFP and

DO INTEND TO RESPOND WITH A PROPOSAL ____X____

DO NOT INTEND TO RESPOND WITH A PROPOSAL _____

AGENCY/ORGANIZATION/INDIVIDUAL **SECURUS Technologies, Inc. through its wholly owned subsidiary Evercom Systems, Inc.**

ADDRESS **14651 North Dallas Parkway, Suite 600**
Dallas, Texas 75254

SIGNATURE _____ DATE **January 24, 2008**

John J. Viola
Vice President and General Manager of Correctional Services

STATE OF ALASKA RFP NUMBER 2008-2000-7549
AMENDMENT NUMBER ONE

RETURN THIS AMENDMENT TO THE ISSUING OFFICE AT:

Department of Corrections
Division of Administrative Services
P. O. Box 112000
Juneau, AK 99811-2000

THIS IS NOT AN ORDER **DATE AMENDMENT ISSUED: December 19, 2007**

RFP TITLE: Inmate Telephone System for State of Alaska Correctional Institutions

RECEIPT OF PROPOSALS DATE AND TIME: Janaury 15, 2008, AT 2:30 P.M. ALASKA PREVAILING TIME.

The following changes/additions are required:

Change Section 5.10.8 of the RFP to read:

5.10.8 The Offeror shall provide a percentage of the gross revenues for all calls. The Offeror shall not deduct fraudulent, uncollectible or un-billable calls , Local Exchange Carrier (LEC) access, LEC or long distance usage, maintenance or any costs of running the ICS, from the gross revenues for all calls prior to paying the percentage rate to the DOC. In other words, the percentage rate shall be based upon gross call cost including per call surcharges and per minute charges, not the net after expenses. The Offeror is responsible for collecting all revenue from the called party for collect calls billed.

Change Section 5.29.10 of the RFP to read:

5.29.10 The Offeror shall provide a percentage of the gross call cost for all answered prepaid calls as a monthly commission fee to DOC. The Offeror shall not deduct fraudulent, un-collectible or un-billable calls, Local Exchange Carrier (LEC) access, LEC or long distance usage, maintenance or any costs of running the ITS, from the gross call cost for all answered prepaid calls prior to applying the commission percentage rate for DOC. In other words, the commission percentage rate shall be based on gross call cost including per call surcharges and per minute charges, not the net after expenses.

Change Section 7.05 of the RFP to read:

Overall, a minimum of 60% of the total evaluation points will be assigned to cost. The cost amount used for evaluation may be affected by one or more of the preferences referenced under Section 2.13.

Converting Cost to Points

The cost proposal providing the largest percentage of generated revenues to the State will receive the maximum number of points allocated to cost. The point allocations for cost on the other proposals will be determined through the method set out in Section 2.15.

STATE OF ALASKA RFP NUMBER 2008-2000-7549
AMENDMENT NUMBER ONE

In order for your proposal to be considered responsive for this amendment, in addition to your original proposal, must be received by the issuing office of the Division of Administrative Services prior to the date and time set for receipt of proposals.

Jack Gregson
Contracting Officer
PHONE: (907) 465-3399
TDD: (907) 465-3274
FAX: (907) 465-2006

SECURUS Technologies, Inc. through its wholly owned subsidiary Evercom Systems, Inc.
NAME OF COMPANY

SIGNATURE

January 24, 2008
DATE

John J. Viola
Vice President and General Manager of Correctional Services

STATE OF ALASKA RFP NUMBER 2008-2000-7549
AMENDMENT NUMBER TWO

Department of Corrections
Division of Administrative Services
Address 802 3rd Street, Room 221
Douglas, Alaska 99824

THIS IS NOT AN ORDER **DATE AMENDMENT ISSUED: January 8, 2008**

RFP TITLE: INMATE TELEPHONE SYSTEMS FOR ALASKA CORRECTIONAL INSTITUTIONS

RFP OPENING DATE AND TIME: 2:30 p.m., Alaska prevailing time on Wednesday, January 23, 2008.

This amendment is for informational purposes only and need not be returned to the State.

1. **Change time and date of receipt of the RFP to 2:30 p.m. Alaska prevailing time on Wednesday, January 23, 2008.**

Jack Gregson
Contracting Officer
Phone: (907) 465-3399
TDD: (907) 465-3274
FAX: (907) 465-2006

SECURUS Technologies, Inc. through its wholly owned subsidiary Evercom Systems, Inc.
NAME OF COMPANY

SIGNATURE

January 24, 2008
DATE

John J. Viola
Vice President and General Manager of Correctional Services

STATE OF ALASKA RFP NUMBER 2008-2000-7549
AMENDMENT NUMBER TWO

Department of Corrections
Division of Administrative Services
Address 802 3rd Street, Room 221
Douglas, Alaska 99824

THIS IS NOT AN ORDER **DATE AMENDMENT ISSUED: January 16, 2008**

RFP TITLE: INMATE TELEPHONE SYSTEMS FOR ALASKA CORRECTIONAL INSTITUTIONS

RFP OPENING DATE AND TIME: 2:30 p.m. , Alaska prevailing time on Wednesday, January 30, 2008.

This amendment is for informational purposes only and need not be returned to the State.

1. **Change time and date of receipt of the RFP to 2:30 p.m. Alaska prevailing time on Wednesday, January 30, 2008.**

Jack Gregson
Contracting Officer
Phone: (907) 465-3399
TDD: (907) 465-3274
FAX: (907) 465-2006

SECURUS Technologies, Inc. through its wholly owned subsidiary Evercom Systems, Inc.
NAME OF COMPANY

SIGNATURE

January 24, 2008
DATE

John J. Viola
Vice President and General Manager of Correctional Services

Attachment M

Prepaid Calling Cards

PREPAID CALLING CARDS *Inmate Calling Program*

Facilities are always in need of increased communications capabilities for detainees and friends and family members. Prepaid calling cards provide an alternative calling method for families needing to budget their cost of calls and open up another vehicle for communication. Unfortunately, traditional prepaid calling programs are often limited to friends and family members who are able to open prepaid billing accounts.

Prepaid calling cards provide an alternative calling method that offer numerous benefits for the facility, detainee and friends & family members.

SECURUS' prepaid calling cards create another communication opportunity that assists in the operational efficiencies of your facility and provides you with complete administrative and investigative control of all calling activity. Because SECURUS' prepaid calling cards can be sold as a commissary item, your staff incurs little or no additional administrative requirements.

SECURUS was the first to provide a complete prepaid calling card system, designed with features and benefits focused exclusively on the Correctional and Law Enforcement industry.

PROGRAM BENEFITS

- Increased economic benefits
- Complete investigative and administrative control
- International calling to over 200 countries
- Real time account status:
  - Number Blocking and Un-blocking
  - Reports on Call Traffic
  - Account Balance Updates
  - Call Detail History by PIN
  - Call Complaint History by PIN
  - Optional notification that the call originated from a correctional facility
- Interfaced to SECURUS' Inquiry Center for real time PIN, updates for:
  - Customer Support
  - Blocks and Un-blocks
  - Reporting
  - No refunds required for released detainee's – all remaining prepaid minutes are usable upon release via 800# from any phone in the USA
  - Provides an alternative calling method for families needing to budget their cost of calls

SPECIAL PROGRAMS

Indigent Prepaid Calling

- Facilities can now provide a lower cost alternative for indigent obligations

Reward Program

- Trustee programs
- Rewarding good behavior
- Builds detainee self-esteem
- Eliminates transferring detainees to make mandated calls
- Effective management tool
- Additional funding source

PROGRAM HIGHLIGHTS

- Card denominations range from $5 to $30 with a minimum purchase requirement of $150
- No operator surcharge
- All US call rates are a flat rate per minute; International rates vary

To speak to a Prepaid Calling Cards Specialist contact us at :

866.229.9286

only@securustech.net

M6028