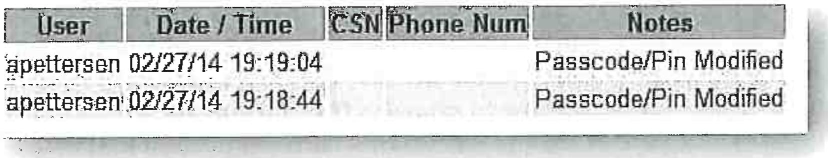


User	Date / Time	CSN	Phone Num	Notes
apettersen	02/27/14 19:19:04			Passcode/Pin Modified
apettersen	02/27/14 19:18:44			Passcode/Pin Modified

Changes Logged in the Inmate Profile

3.11 SYSTEM RESTRICTION, FRAUD CONTROL AND NOTIFICATION REQUIREMENTS

3.11.1 The security and confidentiality of inmate-placed telephone calls is of critical importance. Security features, which prevent unauthorized access to any information held by the vendor, will provide for restriction to the ITS, fraud control for prevention purposes, and notification capabilities for attempted security violations or breaches. Secure access to the ITS will be maintained at all times. The ITS will have security capabilities that include, but are not limited to:

3.11.1.1 Each completed call from the ITS, except registered attorney telephone calls, will include a pre-recorded announcement that the call is subject to monitoring and recording. The pre-recorded announcement will be random, but no less than one (1) time within the first ten (10) seconds of the call and at a minimum of three (3) times in a 30 minute telephone call.

CenturyLink has read, understands and will comply.

CenturyLink has provided random voice overlay announcements to NDOC for the last six years. The standard voice prompt is: "This call is from a correctional facility, and is subject to monitoring and recording."

The announcement content can be customized, along with the announcement volume and frequency.

3.11.1.2 The vendor will be able to detect unusual or suspicious number sequences dialed or dialing patterns, which the ITS identifies as possible attempts to commit fraud.

The vendor must briefly describe how the ITS will perform and/or prevent such fraudulent dialing attempts.

CenturyLink has read, understands and will comply.

For 3.11.1.2 and 3.11.1.3, the first line of defense against such fraudulent calling patterns is "thresholding". Thresholds are managed for both the inmate and the called party. On the inmate side, thresholds can be set to manage dialing patterns, where the ITS detects and prevents repetitive calling to the same number, a large number of calls within a specified timeframe, or

excessive call attempts that result in hang-up before call connection. On the called party side, the ITS can detect and prevent excessive calls to the same number, and excessive calls from multiple inmates – all of which may indicate fraudulent calling. All such threshold parameters exist in the ITS today. Most can be modified by authorized NDOC; for any that must be changed at the System Admin level, CenturyLink is happy to change the parameters at no cost, upon request of the NDOC.

The second line of defense against fraudulent dialing patterns is a new feature, Call Pattern Analysis. Call Pattern Analysis, used on conjunction with thresholds, can identify and prevent potentially fraudulent dialing attempts. A complete description of Call Pattern Analysis follows.

Call Pattern Analysis
The ITS can be equipped with a robust analytical system that enables correctional staff to quickly and easily identify calls of interest that are most likely to provide actionable intelligence among the thousands of inmate conversations recorded each month. Call Pattern Analysis works by analyzing the associations between inmates, called parties, and even other inmates and – most importantly – by identifying changes in these associations or calling patterns that could indicate illicit activity.

Calling patterns are naturally established as the result of inmate and called party schedules and preferences. For instance, an inmate is usually familiar with each called party's work schedule and will avoid calling during certain times (such as weekdays, for example) when that person is usually at work. To increase the likelihood of having their call answered, the inmate will naturally make a habit of calling in the evening or over the weekend.

While legitimate changes in pattern do sometimes occur – such as when a change is made in the called party's work schedule – disruptions to normal patterns can also be an indicator that illicit activity is occurring.

For example, if a pattern of regular communication exists between a particular inmate and a called party, and then communication suddenly ceases altogether, the absence of calling could indicate that the inmate has obtained the use of an illegal cell phone, on which he or she is making these phone calls. If calling to this telephone number suddenly resumes on the regular schedule, but it is a different inmate who is placing the calls, this could indicate that the called party is merely facilitating communications to the outside world and possibly assisting in the completion of illegal communications.

Call Pattern Analysis identifies relationships and calling patterns among inmates, called parties, and even other inmates. Call Pattern Analysis then detects subtle and dramatic changes in these relationships and calling patterns to identify calls, inmates, and called numbers as suspicious. Call Pattern Analysis will increase the productivity and efficiency of your investigative staff by automatically identifying calls of interest that are most likely to provide actionable intelligence.

Detailed queries can be structured – based upon timeframe, called number and\or inmate PIN – to help investigators pinpoint calls of interest, such as:

- ***Phone numbers called by multiple inmates***
- ***Phone numbers that appear on multiple inmates' PAN lists***
- ***Phone numbers that appear on an inmate's PAN list but are never called***
- ***Frequently called numbers***
- ***Sudden absence of an inmate's regular calling***

- ***Sudden absence of calling to a particular number***
- ***Changes in regular calling times/days***
- ***Increase in inmate calling over a finite period***
- ***Decrease in inmate calling over a finite period***
- ***Increase in calling to a particular BTN over a finite period***
- ***Decrease in calling to a particular BTN over a finite period***
- ***Transfer of communication patterns from one inmate PIN to another inmate PIN***

Investigators can use this information to isolate call recordings of interest. Or, they can use the ITS's custom reporting tools to create detailed reports containing particular data of interest – for example:

- ***A list of all numbers called by more than one inmate within a specified timeframe***
- ***A list of all calls attempted by a particular inmate during a designated timeframe***
- ***A list of all telephone stations used to dial a particular telephone number.***

The System's flexible reporting application allows investigators to create custom queries based upon any combination of the data that is collected for each and every phone call, and to save these custom queries locally or globally in order to quickly run the reports again over future timeframes.

3.11.1.3 The proposed ITS will provide a call alert and notification feature. An alert is an immediate visible indication of a suspected event that can be set by authorized NDOC staff. A notification is an e-mail or phone call to an identified event selected by authorized NDOC staff. The event can include but is not limited to:

A. A certain inmate placing a call,
B. A certain number is called by an inmate, or
C. A NDOC unauthorized call attempt is made.

The vendor will briefly describe the alert feature proposed with the proposed ITS and the options available to the NDOC.

CenturyLink has read, understands and will comply.

The ITS provides an Alert feature to aid investigators in up-to-the-minute inmate telephone activity. The ITS alerts can be placed on specific Inmate PINs or specific destination numbers to indicate that the inmate or number is currently involved in a conversation. These alerts can be delivered in the following ways:

- ***Monitoring Alerts - The ITS can call an investigator on their telephone (or cell phone) and once provided with an approved pass code can immediately patch the investigator into a the ITS monitoring session for almost instantaneous access to inmate activity. This capability is silent and undetectable by the inmate and the called party.***

- ***Email/SMS Alerts – The ITS can send email or SMS message to an administrative workstation or any public email address when an alert is triggered.***

- ***Paging Alerts* - *The ITS can issue numeric messages to paging services to alert an investigator.***

Furthermore, investigators can set the ITS to automatically transfer calls to them for monitoring wherever they may be by using CenturyLink's "Find Me, Follow Me" service. "Find Me, Follow Me" allows call alerts to phone multiple investigator telephone numbers (such as an office number, cell number, and home number), trying each number in succession until the investigator answers and enters the correct access code; this feature dramatically increases the probability than an investigator will be located and can monitor a call of interest while it is still in progress.

<u>Best-in-Class Solution: Find Me, Follow Me</u>

This feature, currently in use at NDOC, enables a single alert to try more than one number to contact an investigator

3.11.1.4 The vendor will be able to identify and report, 3 way or conference calling and call forwarding. The vendor must have features that allow authorized NDOC staff options to manage identified calls. If authorized NDOC staff chooses to disconnect the call, the ITS will interject a message stating "This call is being disconnected in ten (10) seconds".

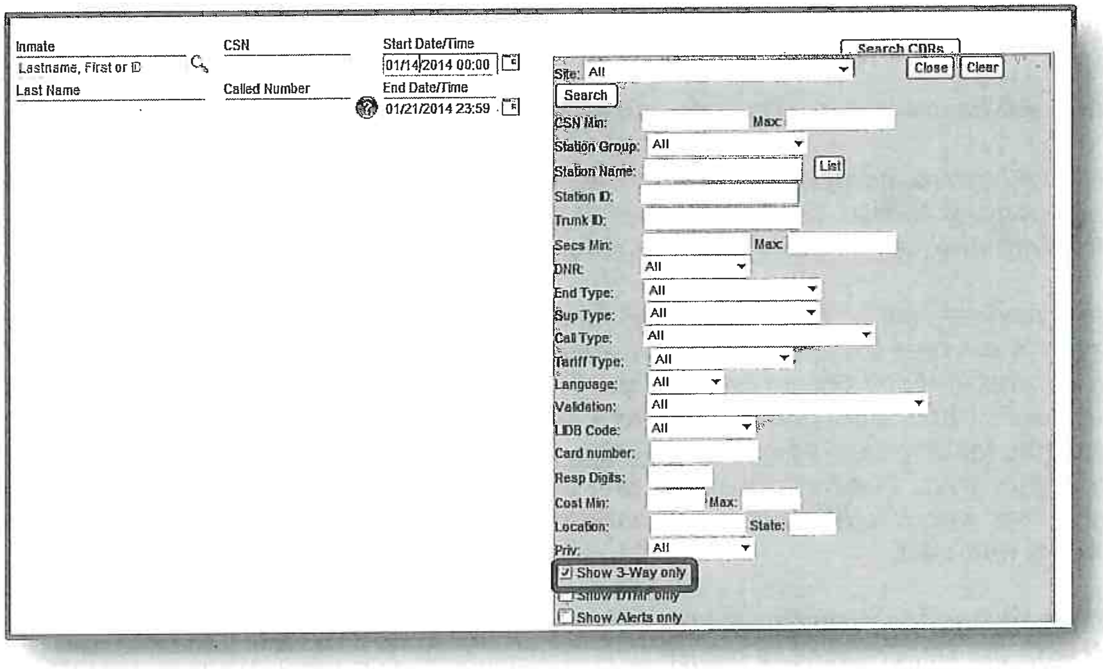
CenturyLink has read, understands and will comply.

CenturyLink has read, understands and will comply. The ICS automatically detects attempts by destination parties to connect, or forward, calls to a third party. These detection features have highly configurable parameters for changing the sensitivity to accommodate the requirements of each installation. When a three-way call attempt is detected, the system can:

- ***Flag the call for investigation***
- ***Flag the call for investigation, and play a warning message to the inmate and called party***
- ***Flag the call for investigation, play a notification to the inmate and called party, and terminate the call***

The system will be programmed to take whichever action NDOC prefer from the list above. This action is also configurable by called number, for example, not taking action on attorney calls (which may be transferred from a receptionist). CenturyLink highly recommends allowing the call to proceed, because valuable investigative data can be found by reviewing calls that were flagged as three-way attempts.

When the system is configured to terminate a call upon detection of fraudulent use, such as three-way call attempts, a voice prompt is played to both parties on the call upon "sensing" a usage violation. This voice prompt typically informs the parties that fraudulent use has been detected and disconnects the call. The resulting call record is then flagged with this detection and termination for future query and reporting purposes, as shown on the following screen:



Inmate: Lastname, First or ID
Last Name
CSN
Called Number
Start Date/Time: 01/14/2014 00:00
End Date/Time: 01/21/2014 23:59

Site: All
CSN Min: Max:
Station Group: All
Station Name:
Station ID:
Trunk ID:
Secs Min: Max:
DNR: All
End Type: All
Sup Type: All
Call Type: All
Tariff Type: All
Language: All
Validation: All
LIDB Code: All
Card number:
Resp Digits:
Cost Min: Max:
Location: State:
Priv: All
☑ Show 3-Way only
☐ Show DTMF only
☐ Show Alerts only

Call Detail Screen – Report on Suspected 3-Way Calls

Detection of fraudulent use can be managed through sensing of call progress, DTMF tones from either party on the call, and extended silence periods during the call. The success of this DTMF or extended silence, detection is very reliable. However, it does not always indicate call-forwarding or three-way call set up. Many correctional facilities with full-channel recording have found that a Three-Way Call Deterrent Policy is much more effective. With such a policy, the deterrent to making three-way calls is the inability for inmates to make future calls. Unlike the old methodology, which only blocked or cut off the called party, the inmate was still able to call back to the called party and try numerous ways to exploit the system until they succeeded.

The sensitivity of detection settings is also configurable so that parameters can be set to optimize performance.

Standard three-way activity reports from the ICS system can facilitate investigations into suspected three-way call attempts. The three-Way Attempts report lists all three-way call attempts detected, along with all associated call detail information. The Top 25 three-Way Destination Numbers shows the top 25 called numbers that triggered three-way call detection.

Proprietary / Confidential Information Redacted for Call Forwarding Detection, included in Part I B – Confidential Technical Proposal.

3.11.1.5 Optional Requirement - Vendors will provide technology information on their ability to detect the presence of cell phones within a facility. This can be done through the vendor's company or in conjunction with a subcontractor. Provide a separate line in the proposal cost section ***Attachment P, Cost Commission Proposal.***

CenturyLink has read, understands and will comply.

As NDOC is well aware, contraband cell phones are one of the most critical challenges facing correctional agencies today. Technologies to detect and/or prevent communications to/from these devices are new, as are laws and regulations governing their use.

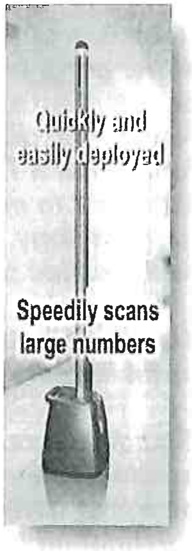
Over the past several years, the CenturyLink team (including our technology partner ICSolutions) has become expert in the technologies and importantly, the laws and regulations involved in contraband cell phone prevention. This includes first-hand knowledge through deployments of Portable Detection Units and a Service Denial installation, in addition to a Managed Access installation. <u>To our knowledge no other provider has this breadth of first-hand experience in this area</u>. The bottom line is that there is no single solution to this issue – each technology brings with it a different combination of effectiveness, operational complexity, legal considerations, and cost.

CenturyLink is pleased to provide a wide array of options to NDOC, and offers to discuss each in more detail with the Department as desired.

<u>Approach #1: Portable Detection Units (CellSense or CEIA USA)</u>

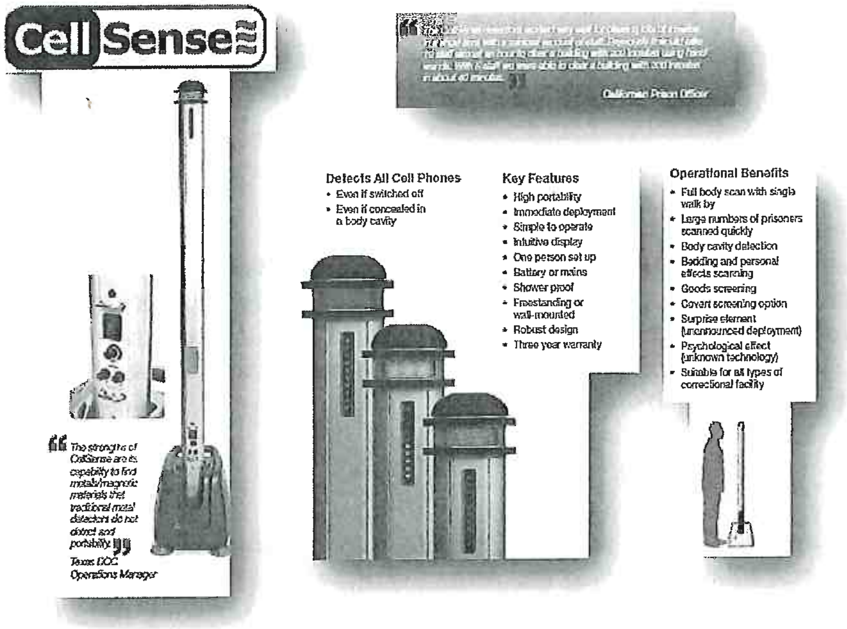
Portable detection units are valuable and cost-effective tools in combating contraband, especially contraband cell phones. These units can be rapidly deployed and remain visible to inmates, or be hidden behind visual barriers for covert operation.

CenturyLink works with both leading providers of this technology – CellSense and CEIA USA – and is able to provide NDOC with either technology, or a combination of both. In fact we recommend an approach where the existing CellSense unit in place today is maintained and complemented by a CEIA USA unit – after an evaluation period the Department could order additional units based on its preference.



<u>CellSense.</u>
As the Department is already aware, CellSense, by MetraSens, is a proven system for detecting the presence of cell phones in or on the body, even if the phone is switched off. It also has the advantage of also detecting other contraband items such as shanks, knives and small blades.

Rapid and un-announced deployment and the ability to scan up to 40 individuals per minute means that it is clearly the most cost effective and flexible cell phone detector available worldwide. It can even be deployed covertly since it has the ability to scan through walls.



CellSense

“[illegible] With 6 staff we were able to clear a building with 300 inmates in about 40 minutes.”

Californian Prison Officer

Detects All Cell Phones
- Even if switched off
- Even if concealed in a body cavity

Key Features
- High portability
- Immediate deployment
- Simple to operate
- Intuitive display
- One person set up
- Battery or mains
- Shower proof
- Freestanding or wall-mounted
- Robust design
- Three year warranty

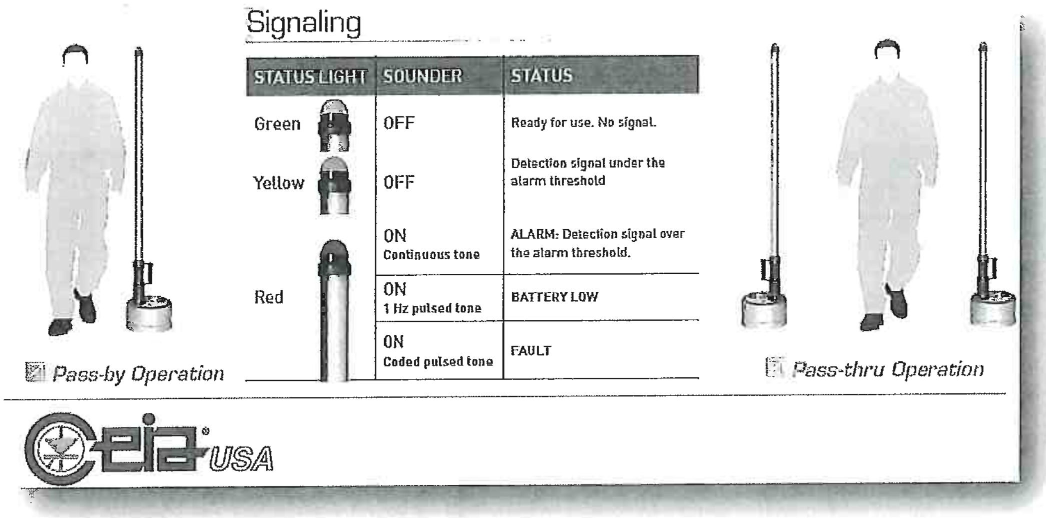
Operational Benefits
- Full body scan with single walk by
- Large numbers of prisoners scanned quickly
- Body cavity detection
- Bedding and personal effects scanning
- Goods screening
- Covert screening option
- Surprise element (unannounced deployment)
- Psychological effect (unknown technology)
- Suitable for all types of correctional facility

“The strengths of CellSense are its capability to find metals/magnetic materials that traditional metal detectors do not detect and portability.”

Texas DOC Operations Manager

<u>CEIA USA.</u>

A similar product is offered by CEIA USA, a leader in metal detection devices. The CEIA unit offers features and portability similar to the CellSense unit, and also like the CellSense unit, has multiple deployments throughout the U.S.



Signaling

STATUS LIGHT	SOUNDER	STATUS
Green	OFF	Ready for use. No signal.
Yellow	OFF	Detection signal under the alarm threshold
Red	ON Continuous tone	ALARM: Detection signal over the alarm threshold.
	ON 1 Hz pulsed tone	BATTERY LOW
	ON Coded pulsed tone	FAULT

Pass-by Operation

Pass-thru Operation

ceia USA

References for both companies are gladly provided by request.

<u>Approach #2: Contraband and Cell Intel Assessment Services</u>

Assessment services, offered through our partner ShawnTech Communications, can be provided in two different methodology that could be used to not only quantify the problem but also

support extraction and investigative efforts. When conducted multiple times at one facility, data available through the assessments can also be used to measure the effectiveness of policies, procedures and extraction techniques implemented to manage contraband mobile devices. These two solutions are 1) Contraband Assessments and 2) Cell Intel (contraband assessments with additional intelligence reporting).

Contraband Assessments

Contraband assessments include an on-site assessment detecting the number of powered on devices for up to two physical locations within one facility. Each "location" is broken down into targeted "zones" providing an indication to the number of powered on contraband devices detected including hardware IDs. The data are used to 1) quantify the extent of the problem with contraband devices and 2) support extraction efforts.

Cell Intel (Contraband Assessments + Intelligence)

ShawnTech's Cell Intel solution provides all of the same information as contraband assessment but also includes additional intelligence data including the phone # dialed and text (SMS) messages from the contraband device detected. The additional intelligence provided facilitates extraction efforts and provides investigative data not otherwise available.

The Cell Intel solution is a unique offering available through ShawnTech. With FCC and carrier approvals, ShawnTech is able to provide the information assuming compliance with state laws.

Requirements

Both solutions (Contraband Assessments and Cell Intel) detect "powered on" mobile devices within the contraband assessment's coverage area. Protocols supported include GSM and UMTS.

Protocol	Carrier Examples	Uses SIM Card?	Notes
GSM – Global System for Mobile Communications (2.5G)	AT&T, T-Mobile	Yes	Popular with offender population due to ease of sharing device and lower costs
UMTS – Universal Mobile Telecommunications System (3G+)	AT&T, T-Mobile	Yes	Popular with offender population due to ease of sharing device and lower costs

The services and deliverables are included per solution as follows:

Item / Deliverable	Contraband Assessment	Cell Intel
Site survey to prepare for assessment	Remote	On-site
Legal review to ensure compliance with state laws	N/A	✓

FCC and carrier approvals (STA or equivalent)	N/A	✓
Technicians to setup and configure equipment; operate equipment and conduct assessment	Up to 16 hours / tech	Up to 24 hours / tech
Data analysis	✓	✓
Report delivered to Customer electronically within seven (7) business days following on-site assessment	✓	✓
Report Briefing to Customer via conference call and/or webinar	✓	✓
Report data to include:		
Overview of assessment methodology such as locations and "zones" covered (e.g., housing unit)	✓	✓
Number of powered on devices detected within a specified zone (e.g., housing unit)	✓	✓
Date and time of captured mobile devices	✓	✓
IMSI / SIM or MIN – International Mobile Subscriber Identity / Subscriber Identity Module / Mobile Identification Number	✓	✓
IMEI / HW or pESN – International Mobile Equipment Identity / Hardware ID / pseudo Electronic Serial Number	✓	✓
Carrier – Native carrier (e.g., AT&T, T-Mobile)	✓	✓
RX Level (dBm) – Signal strength, according to mobile device	✓	✓
Band – Configured radio of system that captured mobile device	✓	✓
Name – Name / owner of known mobile devices (e.g., Warden, Test devices, etc)	✓	✓
Originator – Virtual phone number assigned to the device by the RAN (phone # is unknown)		✓
Recipient – Phone number dialed by the user of the device		✓
Time Rx – Date and time message was sent from device		✓
Receiver IMSI / Sender IMSI – IMSI of the device receiving the message and sending the message, respectively		✓
Receiver MSISDN / Sender MSISDN – Mobile Subscriber Integrated Services Digital Network-Number for receiver and sender, respectively		✓
Ack – Acknowledgement by system / device		✓
Operation – Text field designation defined on system interface		✓
Place – Location name loaded for the operation		✓
Original message – Content of actual message sent		✓

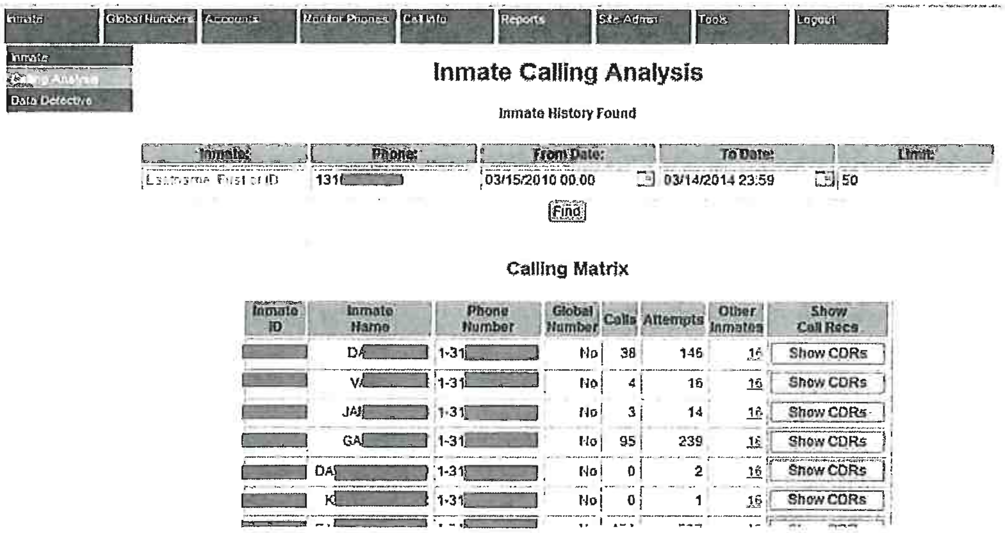
Approach #3 – Cellebrite extraction units

Cell phone extraction units are not used to detect contraband devices, but rather extract information from contraband devices that are captured by Department personnel. When considering the rich investigative data available from the extraction unit, inmates are deterred from bringing in contraband devices.

CenturyLink offers Cellebrite's UFED Ultimate all-in-one mobile forensic solution. UFED Ultimate performs physical, logical, and file system extractions of cell phones – performing a complete data extraction of existing, hidden, and deleted phone data, including call history, text messages, contacts, email, chat, media files, geotags, passwords, and more.

Ultimate also includes UFED Physical Analyzer, which highlights the most critical components of an extracted phone's memory data, making navigating through the data easier and more flexible than ever. Users can generate reports, print them, and/or save them to their computer in PDF, HTML, XLS, and XML formats.

The exact deployment depends on NDOC's preference. CenturyLink offers use of its NV-based service personnel to perform extractions and upload data to our secure database. Alternatively and recognizing the Department's policies regarding access to sensitive data by non-Department personnel, CenturyLink offer to simply provide device(s) and develop an interface to NDOC's preferred database. Reports can then be custom-developed for numbers called from the inmate telephone system, using existing reporting capabilities within the Enforcer.



Inmate Calling Analysis

Inmate History Found

Inmate:	Phone:	From Date:	To Date:	Limit:
Lastname, First or ID	131[redacted]	03/15/2010 00:00	03/14/2014 23:59	50

Find

Calling Matrix

Inmate ID	Inmate Name	Phone Number	Global Number	Calls	Attempts	Other Inmates	Show Call Recs
[redacted]	D[redacted]	1-31[redacted]	No	38	146	16	Show CDRs
[redacted]	V[redacted]	1-31[redacted]	No	4	16	16	Show CDRs
[redacted]	JA[redacted]	1-31[redacted]	No	3	14	16	Show CDRs
[redacted]	GA[redacted]	1-31[redacted]	No	95	239	16	Show CDRs
[redacted]	DA[redacted]	1-31[redacted]	No	0	2	16	Show CDRs
[redacted]	K[redacted]	1-31[redacted]	No	0	1	16	Show CDRs

Inmate Calling Analysis Screen
(for searching called numbers extracted from Cellebrite Unit)

<u>Approach #4 – Cell phone location (CellBusters)</u>

CellBusters' Zone Protection and Management system provides information on contraband cell phone use in a given radius, providing both the location (within the given radius) and the number of phones in use.

The Zone Protector™ unit (shown right) has an approximate 100

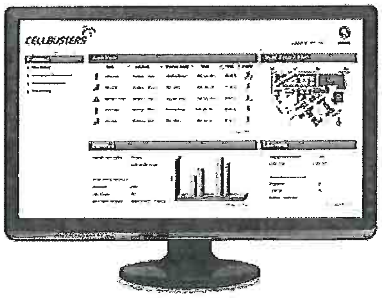
foot radius and can detect cell phones, WIFI devices, or other mobile devices (CDMA, GSM, 3G, 4G, LTE, and others), while known frequencies such as officers' two-way radios can be filtered out. In addition, because device and/or subscriber-specific information is not provided, legal concerns regarding privacy are essentially eliminated.

Implementation

Multiple power (battery, USB, AC adapter) and networking options (wireless or LAN-based) are available to minimize infrastructure time and cost.

Oversight and ongoing maintenance

Zone Protector units can be coupled with Zone Manager software to provide control and visibility of policy breaches, including statistics and reporting from devices over encrypted and secure connections. The software enables DOC staff to measure the effectiveness of policies using a simple web-based application.



Approach #5 – Remote Detection and Control through Service Denial

This service, offered by CellAntenna, bridges a gap between direct detection methods such as #1 above and automated control methods such as #3 below. The typical installation involves a fixed Distributed Antenna System (DAS) within the facility to detect and inventory contraband cell phone units. A portable Cell Phone Controller (CPC) – the most costly part of the solution – is then transported between facilities to perform sweeps. Once the sweep is performed, the inventory of detected contraband units is then sent to the carriers to shut off service to the devices.

Put another way, the service is an "off air" system designed only to capture the serial numbers of cell phones found inside a facility. Once captured, the numbers are refined to remove those that belong to authorized users, and the rest of the list, sorted by carrier, is submitted to the carriers for removal of the offending cell phone subscription from their system. In this way the service is designed by be used as a more affordable control service, with the only permanently installed hardware being the DAS.

The active part of the system (the CPC) is only placed at the facility for a short period of time (3-4 days), capturing as many cell phones that are in use during the period as possible. The unit can then moved to another facility where it is used in the same manner. The estimated effectiveness of the system approaches 95% over a period of four months, where repetitive measures reduce the number of cell phone population at each pass. Since no attack is made by the system, 911 calls are not affected.

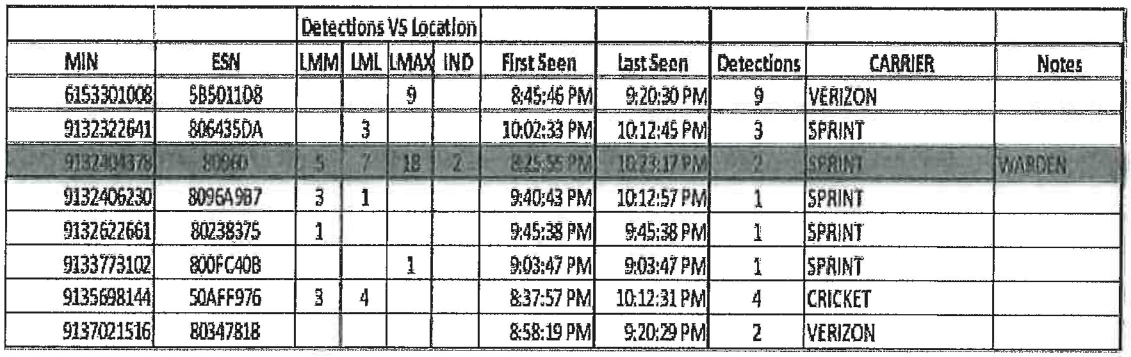
- *Service Delivery – CellAntenna's trained technicians will connect and disconnect the CPC unit*
- *Remote 24/7 monitoring*
- *Duration - Based on size of a facility, estimate three days of equipment deployment onsite for each visit*

- ***Target area = Housing units - as the majority of contraband handsets are used inside the housing units***
- ***Deployment - Fixed antenna system installed inside of housing units – estimated 90% capture rate/visit***

Implementation

The infrastructure required by the Guardian service is a DAS, a group of small antennas throughout the facility connected through copper and fiber wiring back to a central hub. The portable CPC connects to the hub to perform regular analysis

Installation of the DAS typically takes approximately 3-4 months, with timeframes varying according to the wiring/conduit infrastructure already in place (if use is allowed), the amount of inter-building cabling needed, availability of security escorts, and other factors. Please note that infrastructure installation will impact operations, although our experience with the installation in Texas should minimize interruptions. In any case, installation of infrastructure will not impact the inmate telephone system.



		Detections VS Location								
MIN	ESN	LMM	LML	LMAX	IND	First Seen	last Seen	Detections	CARRIER	Notes
6153301008	5B501108			9		8:45:46 PM	9:20:30 PM	9	VERIZON	
9132322641	806435DA		3			10:02:33 PM	10:12:45 PM	3	SPRINT	
9132404378	80960	5	7	18	2	8:25:55 PM	10:23:17 PM	2	SPRINT	WARDEN
9132406230	8096A9B7	3	1			9:40:43 PM	10:12:57 PM	1	SPRINT	
9132622661	80238375	1				9:45:38 PM	9:45:38 PM	1	SPRINT	
9133773102	800FC40B			1		9:03:47 PM	9:03:47 PM	1	SPRINT	
9135698144	50AFF976	3	4			8:37:57 PM	10:12:31 PM	4	CRICKET	
9137021516	80347818					8:58:19 PM	9:20:29 PM	2	VERIZON	

Oversight and ongoing management

Ongoing maintenance for the service is straightforward. Following installation of the DAS, a portable CPC is brought to the DAS hub to perform analysis over a prescribed time period – typically three to four days at random intervals. The CPC detects and identifies contraband handsets inside the facility, in addition to their general location and captures their unique serial number information (IMEI/IMSI – ATT/T-Mobile, IMSI – ATT, UMTS and ESN/MIN – Sprint/Verizon). The captured cellular handset information can be used by investigators and criminal justice practitioners to:

- ***Facilitate targeted searches***
- ***Aid investigators and cell carriers in determining a chain of custody for the detected/indentified handsets in an effort to determine how contraband handsets and SIM cards are being smuggled into the correctional facilities.***
- ***Have the detected handset's service disconnected by the subscribing carrier (passive service denial).***

Working with staff, CellAntenna and/or CenturyLink staff would complete a detailed inventory of detected devices along with the times of detection, general location, and device identification information to send to carriers for disconnection. The following screen illustrates the information captured by the system:

Clearly the most complex piece of the ongoing managerial process is working with the carriers to disconnect service. CellAntenna is currently installed in a privately-owned facility through which processes and standards for service disconnection of individual cell phones are being finalized with carriers.

Updating hardware/software

Updating of hardware/software is straightforward. All the intelligence of the system is housed in the portable CPC unit, which is stored at a central location. As new capabilities are introduced, the CPC is automatically updated with the latest software. An important note: these new capabilities could also include jamming of cell phone signals when and if legalized – CellAntenna is a recognized leader in precision jamming technology.

Approach #6 – Remote Detection and Control through "Managed Access"

Through our relationship with ShawnTech Communications, CenturyLink offers the C5 Managed Access solution to NDOC. CenturyLink notes that it recently chose the C5 solution as its preferred Managed Access solution following a lengthy and structured Solicitation process. The specifications of that Solicitation are available to NDOC at its request.

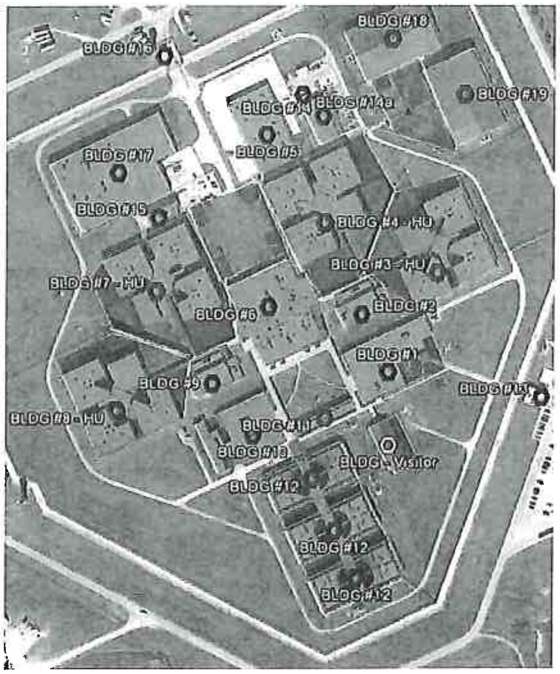
Managed Access uses a DAS similar to the Guardian service described above, and attaches to it a group of cellular base stations that automatically control communications from contraband devices. Several companies provide Managed Access systems and CenturyLink is able to work with any of them. However, the response below is specific to the ShawnTech C5 System that CenturyLink is installing at the Texas Department of Criminal Justice, which was selected as part of a structured procurement managed by CenturyLink.

The ShawnTech solution, "Secure Communications/Mobile Device Interdiction", is based on the ability to provide these features:

- ***Detect the operation of an illicit cellular device within a defined secure wireless area***
- ***Record relevant information for each illicit device, such as electronic serial numbers, make/model of phone, time/day of detection, and subscriber information***
- ***Prevent illicit devices from communicating with the cellular network***
- ***Provide easy-to-use tools for tracking activity, alarming tampering events, etc.***

ShawnTech's solution consists of six modes of operation:

- ***Network Analysis***
- ***Intelligent Detection***
- ***Location Identification***
- ***Managed Access***
- ***Redirection of Service***
- ***Denial of Service***



The System is designed to operate 24/7, and provides control of mobile devices within ShawnTech's secure communication infrastructure, ensuring maximum capturing and controlling of unauthorized devices within the defined coverage area. The System will allow authorized devices (based on a device's ID and SIM numbers) and all 911 calls to communicate and place calls.

In active mode, the System takes control of all powered on mobile devices within the defined secure area and verifies whether the device is authorized. For unauthorized devices, the System will proactively take control of the device and direct it to a Trojan control channel. The device will be held, it will not continue to scan the carrier network.

The System processes multiple formats simultaneously and detects any currently operating wireless service for voice, text, and data communications within the secure area, and is an independent System which does not interface with the commercial carrier's network. It also does not require ongoing carrier support with the exception of Spectrum Agreements (which ShawnTech currently has completed).

Oversight and management

ShawnTech has developed several security measures and preventative maintenance procedures to ensure the System is secure and functional. These measures include monitoring at several layers so that authorized personnel and ShawnTech's NOC technicians are notified of issues or compromised systems.

System monitoring logs include system shutdowns/power on, login access (failures and successes), IP address of remote system, and other data. The date and time of the incident, person reporting or resolving the incident, and final resolution notes must be recorded. Staff can enter notes and observations, and the logs can be accessed by PADOC staff at any time.

There are four emergency shut-off procedures for the System. All emergency shutdown procedures will be logged by the System with the ability to alert key personnel via text and/or e-mail messages. These alerts can occur periodically if desired (i.e. every 15, 30, 45, 60 minutes) until the System resumes normal operation. ShawnTech NOC technicians will also be alerted immediately and will initiate established monitoring procedures which may include calling a designated point of contact (POC) if desired.

The hardware elements of the System's base station transceivers, as well as enclosures and power components, are packaged in tamper-resistant and tamper-evident cases.

The System is capable of scanning the active carrier networks in the area and comparing the results to previous results. Any change will be investigated, and any required change to communication channels will be implemented.

Updating hardware/software

The System utilizes a modular design, so system elements such as base stations can be added or replaced easily. The System is scalable and configurable, and the modular nature of the System reduces cost and complexity by simplifying the System configuration requirements.

The System is designed to ensure that future cell phone carrier technologies are easily accommodated, allowing the System to evolve and adapt through the addition or upgrade of new technologies in the form of replacement or additional base stations and other system elements. A Technology Refresh Warranty is included in the monthly warranty, maintenance, support and operational management service package.

3.12 SYSTEM NETWORK STATUS MONITORING COMPONENT

3.12.1 All the ITS will provide a system network status monitoring component within the ITS.

CenturyLink has read, understands and will comply.

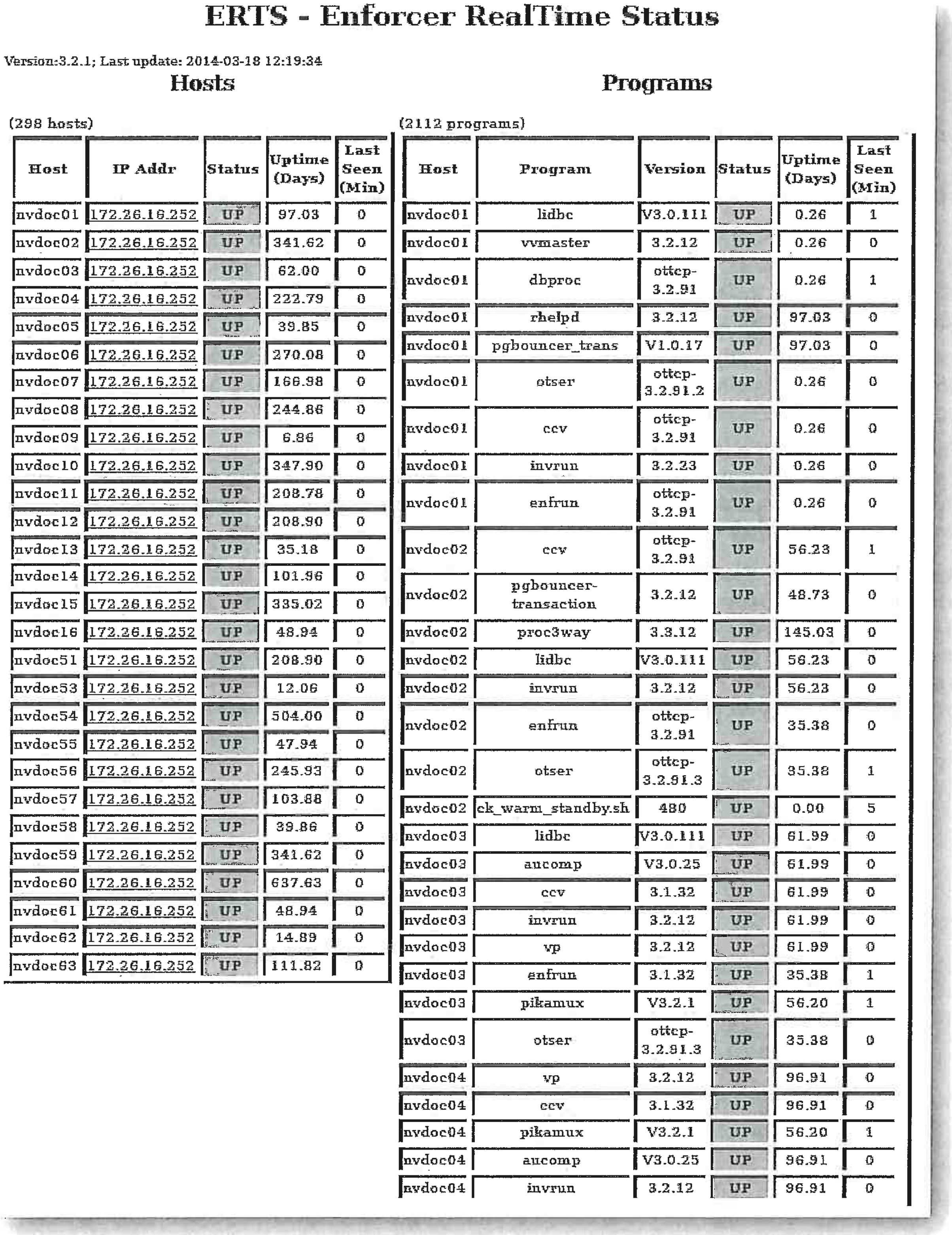
CenturyLink proactively monitors system performance using all of the following methods:

1. Call Volume Activity – The Technical Support Center (TSC) uses the first few months of call activity to identify patterns. Call volume totals are compared daily for variances outside of a defined range (typically a decrease or increase of 15%). An exception report is automatically created for any site showing such variances.

2. Network Availability – Diagnostic routines are constantly being performed to confirm network availability, outgoing trunk status and phone status. Exceptions are automatically reported to the TSC for further investigation and resolution.

3. Variances – Daily call data is compared against normal call activity characteristics for example, the ratio of attempted calls versus. completed calls, percentage of invalid PIN failures, percentage of blocked number failures, etc. Any results outside of the norm will appear on the exception report for further investigation.

4. System Monitoring – System monitoring is part of the fundamental design of all components of the ITS. Key applications send heartbeat messages to the Enforcer Real Time Status (ERTS), our central monitoring system. These heartbeats are recorded in a status database and displayed graphically. ERTS monitors all heartbeats and raises events, should a heartbeat become overdue based on configuration (or policy, in the event specific configuration has not been assigned) to ensure that no missing heartbeats are ignored.



ERTS - Enforcer RealTime Status

Version:3.2.1; Last update: 2014-03-18 12:19:34

Hosts

(298 hosts)

Host	IP Addr	Status	Uptime (Days)	Last Seen (Min)
nvdoc01	172.26.16.252	UP	97.03	0
nvdoc02	172.26.16.252	UP	341.62	0
nvdoc03	172.26.16.252	UP	62.00	0
nvdoc04	172.26.16.252	UP	222.79	0
nvdoc05	172.26.16.252	UP	39.85	0
nvdoc06	172.26.16.252	UP	270.08	0
nvdoc07	172.26.16.252	UP	166.98	0
nvdoc08	172.26.16.252	UP	244.86	0
nvdoc09	172.26.16.252	UP	6.86	0
nvdoc10	172.26.16.252	UP	347.90	0
nvdoc11	172.26.16.252	UP	208.78	0
nvdoc12	172.26.16.252	UP	208.90	0
nvdoc13	172.26.16.252	UP	35.18	0
nvdoc14	172.26.16.252	UP	101.96	0
nvdoc15	172.26.16.252	UP	335.02	0
nvdoc16	172.26.16.252	UP	48.94	0
nvdoc51	172.26.16.252	UP	208.90	0
nvdoc53	172.26.16.252	UP	12.06	0
nvdoc54	172.26.16.252	UP	504.00	0
nvdoc55	172.26.16.252	UP	47.94	0
nvdoc56	172.26.16.252	UP	245.93	0
nvdoc57	172.26.16.252	UP	103.88	0
nvdoc58	172.26.16.252	UP	39.86	0
nvdoc59	172.26.16.252	UP	341.62	0
nvdoc60	172.26.16.252	UP	637.63	0
nvdoc61	172.26.16.252	UP	48.94	0
nvdoc62	172.26.16.252	UP	14.89	0
nvdoc63	172.26.16.252	UP	111.82	0

Programs

(2112 programs)

Host	Program	Version	Status	Uptime (Days)	Last Seen (Min)
nvdoc01	lidbc	V3.0.111	UP	0.26	1
nvdoc01	vvmaster	3.2.12	UP	0.26	0
nvdoc01	dbproc	ottcp-3.2.91	UP	0.26	1
nvdoc01	rhelpd	3.2.12	UP	97.03	0
nvdoc01	pgbouncer_trans	V1.0.17	UP	97.03	0
nvdoc01	otser	ottcp-3.2.91.2	UP	0.26	0
nvdoc01	ccv	ottcp-3.2.91	UP	0.26	0
nvdoc01	invrun	3.2.23	UP	0.26	0
nvdoc01	enfrun	ottcp-3.2.91	UP	0.26	0
nvdoc02	ccv	ottcp-3.2.91	UP	56.23	1
nvdoc02	pgbouncer-transaction	3.2.12	UP	48.73	0
nvdoc02	proc3way	3.3.12	UP	145.03	0
nvdoc02	lidbc	V3.0.111	UP	56.23	0
nvdoc02	invrun	3.2.12	UP	56.23	0
nvdoc02	enfrun	ottcp-3.2.91	UP	35.38	0
nvdoc02	otser	ottcp-3.2.91.3	UP	35.38	1
nvdoc02	ck_warm_standby.sh	480	UP	0.00	5
nvdoc03	lidbc	V3.0.111	UP	61.99	0
nvdoc03	aucomp	V3.0.25	UP	61.99	0
nvdoc03	ccv	3.1.32	UP	61.99	0
nvdoc03	invrun	3.2.12	UP	61.99	0
nvdoc03	vp	3.2.12	UP	61.99	0
nvdoc03	enfrun	3.1.32	UP	35.38	1
nvdoc03	pikamux	V3.2.1	UP	56.20	1
nvdoc03	otser	ottcp-3.2.91.3	UP	35.38	0
nvdoc04	vp	3.2.12	UP	96.91	0
nvdoc04	ccv	3.1.32	UP	96.91	0
nvdoc04	pikamux	V3.2.1	UP	56.20	1
nvdoc04	aucomp	V3.0.25	UP	96.91	0
nvdoc04	invrun	3.2.12	UP	96.91	0

ERTS Status Monitoring for NDOC

Applications are also able to send events to ERTS for action. Any condition which is deemed "not normal" can cause an event to trigger.

All interface programs are capable of sending both heartbeat and event messages to the ERTS system, which means that any regularly scheduled interface which is overdue triggers an event on the centrally monitored status system.

All programs generate detailed log files both for troubleshooting and monitoring, with logs being scraped at least twice per hour for anomalous activity, which is sent to ERTS for processing.

In addition to this passive monitoring which is ongoing, CenturyLink has created the utility "ADTEST," which proactively connects to each analog phone gateway and completes a call to ensure that the gateway is functioning. These tests are run periodically, typically once per hour. Tests are done for both station-side testing and trunk-side testing to ensure there are no problems with the terminating carriers. All negative results from these tests are sent as events to ERTS for logging.

ERTS has various options for event handling notification, including, but not limited to, email, SMS, and user interface alerts.

Our Technical Support and system monitoring teams are responsible for responding to and performing Level 1 support on issues, and escalating both technically and administratively, as appropriate.

3.12.2 The ITS's status monitoring component will, at a minimum:

3.12.2.1 Show graphically, in real-time, the status of the ITS components at each NDOC facility and other locations, to include but not limited to:

A. Calls;
B. Processor equipment;
C. Call monitoring equipment;
D. Call recording equipment;
E. Telephone station equipment; and
F. Network circuit connections.

CenturyLink has read, understands and will comply.

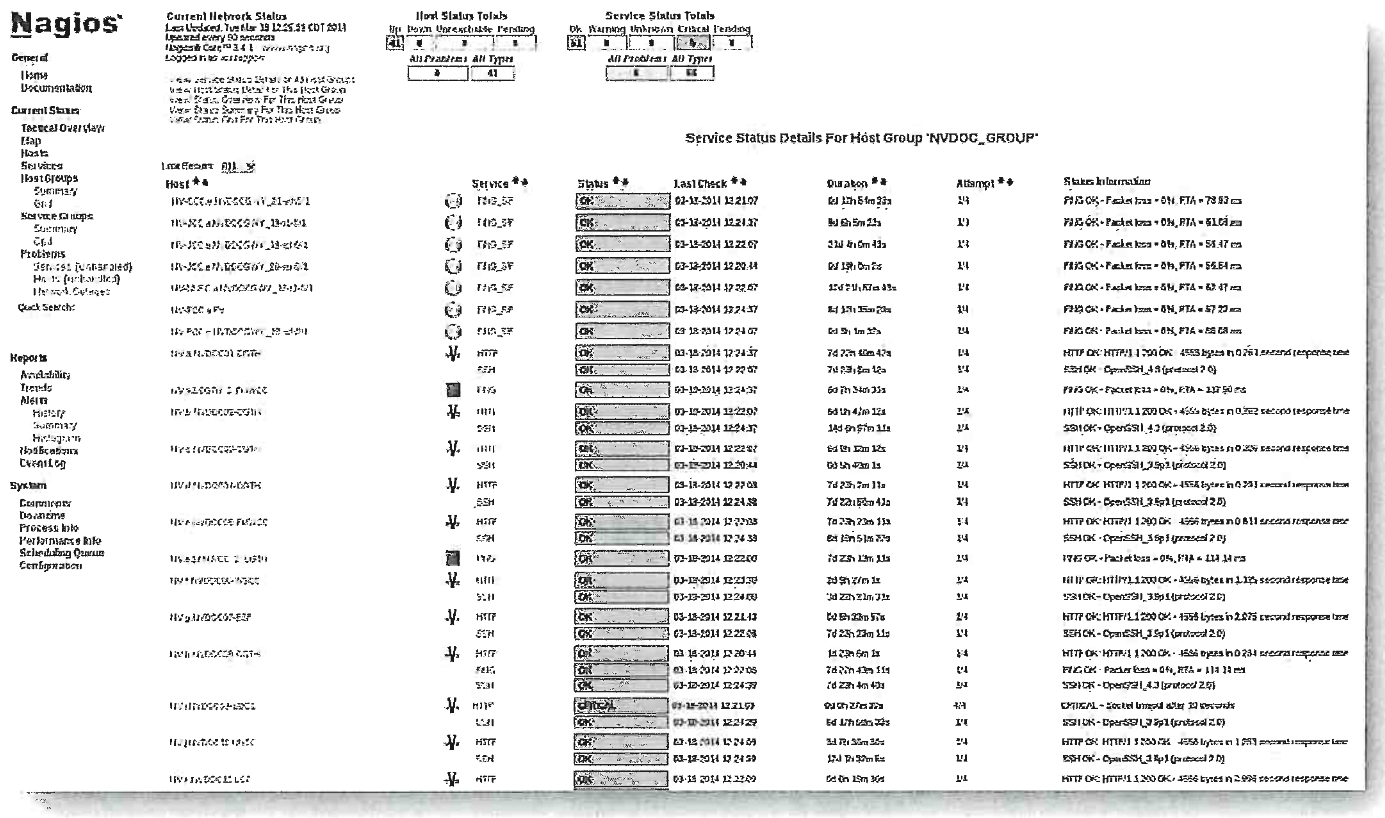
The graphic display is shown in the following subsection.

3.12.2.2 Show component status for the ITS in a minimum of two (2) conditions:

A. "Green" for normal operation; and
B. "Red" for failed operation.

CenturyLink has read, understands and will comply.

The Nagios network monitoring application shows different colors depending on the service event or component status. Green indicates normal operation, while red indicates a critical issue, and yellow indicates that there may be a potential problem.



Current Network Status
Last Updated: Tue Mar 13 12:25:33 CDT 2014
Updated every 90 seconds
Nagios® Core™ 3.4.1 - www.nagios.org
Logged in as [illegible]

Host Status Totals

Up	Down	Unreachable	Pending
41	0	0	0

All Problems	All Types
0	41

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
61	0	0	5	0

All Problems	All Types
5	66

Service Status Details For Host Group 'NVDOC_GROUP'

Host	Service	Status	Last Check	Duration	Attempt	Status Information
[illegible]	PING_SF	OK	03-13-2014 12:21:07	6d 12h 54m 33s	1/4	PING OK - Packet loss = 0%, RTA = 78.93 ms
[illegible]	PING_SF	OK	03-13-2014 12:21:37	9d 6h 5m 23s	1/1	PING OK - Packet loss = 0%, RTA = 61.08 ms
[illegible]	PING_SF	OK	03-13-2014 12:22:07	33d 4h 6m 43s	1/4	PING OK - Packet loss = 0%, RTA = 51.47 ms
[illegible]	PING_SF	OK	03-13-2014 12:20:44	0d 19h 0m 2s	1/4	PING OK - Packet loss = 0%, RTA = 56.84 ms
[illegible]	PING_SF	OK	03-13-2014 12:22:07	12d 21h 57m 43s	1/4	PING OK - Packet loss = 0%, RTA = 82.47 ms
[illegible]	PING_SF	OK	03-13-2014 12:24:37	8d 15h 35m 23s	1/4	PING OK - Packet loss = 0%, RTA = 87.22 ms
[illegible]	PING_SF	OK	03-13-2014 12:24:07	6d 5h 1m 22s	1/4	PING OK - Packet loss = 0%, RTA = 68.68 ms
[illegible]	HTTP	OK	03-13-2014 12:24:37	7d 22h 40m 42s	1/4	HTTP OK: HTTP/1.1 200 OK - 4553 bytes in 0.261 second response time
	SSH	OK	03-13-2014 12:22:07	7d 23h 8m 12s	1/4	SSH OK - OpenSSH_4.3 (protocol 2.0)
[illegible]	PING	OK	03-13-2014 12:24:37	6d 7h 34m 33s	1/4	PING OK - Packet loss = 0%, RTA = 137.50 ms
[illegible]	HTTP	OK	03-13-2014 12:22:07	6d 1h 47m 12s	1/4	HTTP OK: HTTP/1.1 200 OK - 4556 bytes in 0.262 second response time
	SSH	OK	03-13-2014 12:24:37	14d 6h 57m 11s	1/4	SSH OK - OpenSSH_4.3 (protocol 2.0)
[illegible]	HTTP	OK	03-13-2014 12:22:07	6d 6h 32m 12s	1/4	HTTP OK: HTTP/1.1 200 OK - 4556 bytes in 0.269 second response time
	SSH	OK	03-13-2014 12:20:44	0d 5h 42m 1s	1/4	SSH OK - OpenSSH_3.9p1 (protocol 2.0)
[illegible]	HTTP	OK	03-13-2014 12:22:03	7d 23h 2m 11s	1/4	HTTP OK: HTTP/1.1 200 OK - 4556 bytes in 0.231 second response time
	SSH	OK	03-13-2014 12:24:38	7d 22h 59m 41s	1/4	SSH OK - OpenSSH_3.9p1 (protocol 2.0)
[illegible]	HTTP	OK	03-13-2014 12:22:03	7d 23h 23m 11s	1/4	HTTP OK: HTTP/1.1 200 OK - 4556 bytes in 0.811 second response time
	SSH	OK	03-13-2014 12:24:33	8d 15h 51m 22s	1/4	SSH OK - OpenSSH_3.9p1 (protocol 2.0)
[illegible]	PING	OK	03-13-2014 12:22:00	7d 23h 13m 11s	1/4	PING OK - Packet loss = 0%, RTA = 114.14 ms
[illegible]	HTTP	OK	03-13-2014 12:23:30	3d 5h 27m 1s	1/4	HTTP OK: HTTP/1.1 200 OK - 4556 bytes in 1.135 second response time
	SSH	OK	03-13-2014 12:24:03	3d 22h 21m 31s	1/4	SSH OK - OpenSSH_3.9p1 (protocol 2.0)
[illegible]	HTTP	OK	03-13-2014 12:21:43	0d 8h 23m 57s	1/4	HTTP OK: HTTP/1.1 200 OK - 4558 bytes in 2.075 second response time
	SSH	OK	03-13-2014 12:22:03	7d 23h 23m 11s	1/1	SSH OK - OpenSSH_3.9p1 (protocol 2.0)
[illegible]	HTTP	OK	03-13-2014 12:20:44	1d 23h 6m 1s	1/4	HTTP OK: HTTP/1.1 200 OK - 4556 bytes in 0.234 second response time
	PING	OK	03-13-2014 12:22:03	7d 22h 43m 11s	1/4	PING OK - Packet loss = 0%, RTA = 114.18 ms
	SSH	OK	03-13-2014 12:24:39	7d 23h 4m 40s	1/4	SSH OK - OpenSSH_4.3 (protocol 2.0)
[illegible]	HTTP	CRITICAL	03-13-2014 12:21:03	0d 0h 27m 22s	4/4	CRITICAL - Socket timeout after 10 seconds
	SSH	OK	03-13-2014 12:24:29	6d 17h 58m 32s	1/4	SSH OK - OpenSSH_3.9p1 (protocol 2.0)
[illegible]	HTTP	OK	03-13-2014 12:24:09	3d 7h 35m 36s	1/4	HTTP OK: HTTP/1.1 200 OK - 4558 bytes in 1.253 second response time
	SSH	OK	03-13-2014 12:24:39	12d 7h 37m 6s	1/1	SSH OK - OpenSSH_3.9p1 (protocol 2.0)
[illegible]	HTTP	OK	03-13-2014 12:22:09	6d 0h 19m 36s	1/4	HTTP OK: HTTP/1.1 200 OK - 4556 bytes in 2.996 second response time

Nagios Monitoring Screen for NDOC

The network monitoring software is in constant communication with each uninterruptible power supply (UPS), as well. Our UPS Monitor (UPSMon) software continually monitors the status, utility voltage, battery capacity, remaining run-time and UPS Load of every installed ITS nationwide.

The software runs 24/7/365 and automatically sends an email alert to our 24 hour technical support team anytime there is a loss of utility power of any duration, to any ITS device. Most utility power interruptions are very brief. The UPS controlling software also performs a data- save and graceful shut-down of the affected system one minute before primary battery power is exhausted.

In addition to running continuous, automated analyses, technicians can view the status of all UPS units in service at any time from our Network Operations Center (NOC), which proactively monitors the performance of all calling platform equipment.