



WHITE PAPER

with Peer Review Analysis



NO Talk



NO Email



NO Camera



NO Text



NO WiFi



NO Video



TRY SAFETY FIRST
PRISON PROTOCOL TECHNOLOGY
DISABLES 100% OF CONTRABAND CELL PHONES

The following document is a confidential White Paper report on prison protocol technology that disables contraband cell phones that have been illegally smuggled into correctional facilities. The report has been prepared by Try Safety First, Inc. (TSF) - the company responsible for developing the technology. The report also contains a Peer Review Analysis by Corrections Industry Expert John S. Shaffer, Ph.D. The analysis is not to be considered an endorsement by Dr. Shaffer as the TSF technology needs FCC regulation and Carrier participation for full implementation.

PREAMBLE

Any Great General Will Tell You...
The Best Strategy To Hinder An Enemy Is To Cut Off Their Communications

Background: Widespread security and societal threats are emanating from Correctional Facilities across the globe due to contraband cell phones. Almost at will, terrorists and hardened criminals are able to gain possession of illegal cell phones. Ongoing terrorist communications enable recruitment, organizing, plotting and instruction behind bars. Kidnapping, extortion, bribery, witness intimidation, robbery, identity theft, malware attacks, security breaches and other serious crimes are being orchestrated from the inside out due to contraband cell phones.

In an effort to remedy this problem, Try Safety First, Inc. (hereinafter referred to as TSF) has developed and patented unique technology to **COMPLETELY DISABLE ALL** contraband cell phones located in the restricted safety zones of a correctional facility.

The engineering team of Try Safety First designed this technology to be 100% effective. The design was created understanding that regulatory assistance of the FCC and industry compliance of the Wireless Carriers and Handset Manufacturers would be needed. The company is looking to the FCC to take the reins and establish and indoctrinate **a new securitized protocol safety standard** for the wireless industry.

Sound simple? It's not. Technology standardization and migration is never easy! Formidable challenges are anticipated. The White Paper herein describes the technology, the design, the competition, the required testing, the FCC regulation & the industry players in need of compliance for mitigating the challenges for seamless integration of the new safety standard. One that is long overdue!

As you read this paper and you **honestly** ponder if a new safety standard should be created, I simply suggest you think about the continuous criminal behavior and terrorist attacks taking place all over the world. Then ask yourself, is the safety and security of this country worth overcoming a few "temporary" headaches and hurdles to establish this new standard?

John J. Fischer, CEO

Peer Review Excerpt from Corrections Industry Expert

John S. Shaffer, Ph.D.

(See Full Review - Final Page)

This emergent technology solution to the contraband cell phone problem is unique, promising, and worthy of further test and evaluation.

Unlike jamming solutions, the TSF protocol does not indiscriminately terminate cell phones outside of the Restricted Safety Zone. Unlike detection & location systems, the TSF technology does terminate all service to the contraband phones and unlike managed access systems, the TSF technology also terminates all other cell phone functionality (i.e., photos, videos, word processing, Bluetooth, and Wi-Fi hot spots). Bench testing has demonstrated that when the TSF Protocol terminates a cell phone, the phone ceases to function in any capacity. **The cell phone is, in fact, rendered useless.**

Carriers have an existing mechanism (the Regulatory Cost Recovery Charge) that will allow them to recover their investment in public safety and install the technology at every correctional facility in the US. The cost to the individual cell phone user would be nominal.

The next step in the evolution of the TSF protocol technology solution is ...

CONTENTS

White Paper with Peer Review Analysis	1
Preamble & Peer Review Excerpt	2
Contents	3
Overview Of The Problem	4
The Securitized Prison Protocol (The Only Real Solution)	5
5 Step Implementation Process	5
Top 5 Criteria For System & Business Model Development	6
Key Features Currently Being Considered For Development	6
Top 11 Performance Measures For Evaluating System Efficacy	7
Overview Of Competitive Technology Solutions	8
Flow Chart	9
Additional Detail—How It Works	10
PTDP—Protocol Trigger Device For Prisons	11
Prison Example	11
100% EFFECTIVE—TSF Technology Requires FCC Assistance	12
100% COMPLIANCE—Protocol Inclusion	13
100% Control of PTDP's	13
Timeline—Example of 2 Year Protocol Inclusion	14
Cost To Outfit All Correctional Facilities	15
Pilot Test Projections	16
Full Peer Review Analysis by John S. Shaffer, PhD	17

CONTRABAND CELL PHONES - OVERVIEW OF THE PROBLEM



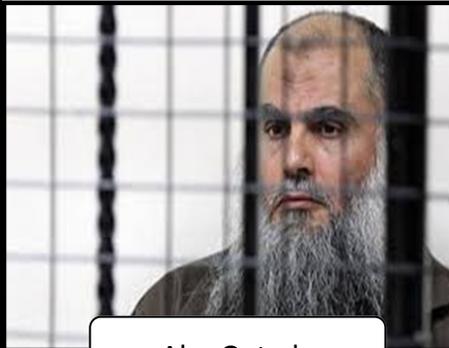
From carrier pigeons to drones, to body cavity to corrupt vendors and staff, cell phones are making their way behind prison walls in very large numbers.

We Live In A Dangerous World and Technology Exacerbates the Problem

Inmates around the world are using contraband cell phones to order contract hits; coordinate escapes; smuggle contraband; intimidate staff, witnesses, and public officials; to orchestrate criminal enterprise; manage gangs; and to remotely direct terrorist activities from behind bars.¹



Abu Bakar Bashir



Abu Qatada

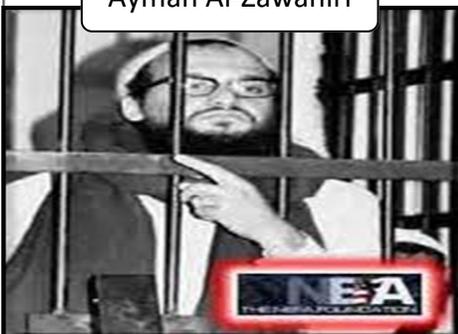


Jemaah Islamiah

According to Peter Neumann, director of London's International Centre for the Study of Radicalization. "Prisons are very important to extremist movements - prison is often the place where it comes together," *Fox News - Prisoners using cell phones coordinated militant attacks from 'Lebanon's Guantanamo'. Jan. 2015.*

The imprisoned terrorists pictured here and many more throughout the world have been found in possession of contraband cell phones during their incarceration. A recent investigation found Henry Okah (leader of the Movement for the Emancipation of Niger Delta who claimed responsibility for Independence Day bombings) with 8 cellphones, 2 chargers, a list of terrorist numbers, and a map in his prison cell. *IOL News South Africa, Feb. 28th 2015.*

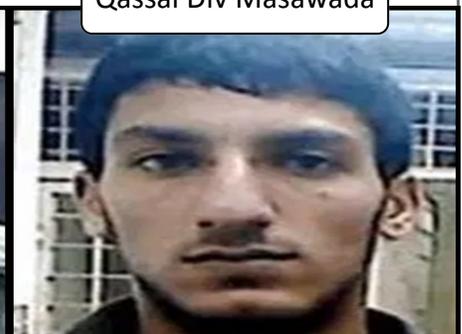
Ayman Al-Zawahiri



Mohammed Zaro



Qassai Div Masawada



¹Shaffer, John S., *Cell Phone Forensics in a Correctional Setting Guidebook*, NIJ Award No. 2010-IJ-CX-K003, 2014.

THE SECURITIZED PRISON PROTOCOL

The Only Real Solution

The reason the TSF Securitized Prison Protocol is deemed to be the only REAL solution is because it is the only system that truly disables all device functionality by turning the device off before the device ever connects to a frequency or accesses the SIM chip. This means No Talk, No Text, No Email, No WiFi, No Pictures, No Video, No Nothing. In essence, the device becomes a paperweight (only exception is 911).

By shutting the device down, the TSF Prison Protocol System even prevents SIM chip data storage for later swapping. Cell Phone SIM chips are very small, can store large amounts of data and are easily transferred between inmates, staff, vendors, and visitors easily permitting concealment of nefarious acts and/or instruction. None of this is possible with the TSF Prison Protocol system—hence, the only REAL system that can actually do what it claims.

How It Works: The complete technology comprises a two part system - one part software and one part hardware. The software (TSF Prison Protocol—TPP) gets embedded into the firmware of all phones in the host country. This is completed with the assistance of the carriers and the manufacturers (See Protocol Inclusion on pg 11 for complete details). The hardware (Protocol Trigger Device for Prisons - PTDP) is strategically placed in specific areas of the prison where cell phone use is prohibited (a Restricted Safety Zone -RSZ). The PTDP acts like a short range beacon (programmable from 1 to 15 meters) and any cell phone in range will become completely disabled. (See PTDP - Beacons on pg 9 for complete details).

Additional Information: It's the only system in the world that scans across the control channel frequency prior to boot-up and also during every algorithmic scan. Prior to granting network access to a phone, the preferred carrier will system verify the phone is security protocol enabled (similar to checking the bill has been paid). The protocol system does not violate the 1934 telecommunications act - it does not interfere with any frequency and emits zero outside molestation. **It is not Big Brother – It Does Not Track, It Does Not Listen and It Does Not Record.**

5 STEP IMPLEMENTATION PROCESS



Step 1 - FCC establishes & indoctrinates new securitized protocol safety standard.

Step 2 - Try Safety First (TSF) provides SDK to all wireless Carriers and Phone manufacturers.

Step 3 - Carriers add Prison Protocol via system update and Mfr's add Protocol during production.

Step 4 - Prisons install PTD's (Protocol Trigger Devices) in select areas (Restricted Safety Zones).

Step 5 - System is activated and all phones in prohibited areas are rendered useless.

Top 5 Criteria TSF Carefully Considered When Developing The Prison Protocol System & Corresponding Business Model

COST	<u>Business model MUST include the Carriers AND generate funds to outfit ALL correctional facilities.</u> Despite having the lowest overall system cost in the industry, Try Safety First has developed a unique business model which: 1) generates funds to outfit <u>ALL</u> correctional facilities (102 Federal Penitentiaries, 1719 State Prisons, 2259 Juvenile Detention Centers, 3283 Local Jails, and 79 Indian Reservation Detention Centers) and 2) creates a new revenue stream for the Carriers for their participation. This allows <u>ALL</u> correctional facilities to fully participate.
CONTAINMENT	<u>Outside interference absolutely CANNOT occur.</u> The TSF Protocol Trigger Device for Prisons (PTDP) beacon can be precisely programmed from 1 to 15 meters thereby eliminating ALL outside molestation.
EFFECTIVENESS	<u>The system MUST disable ALL contraband phone functions (yet still permit emergency 911).</u> What good is a system that doesn't shut down WiFi and Video? A corrections officer then becomes the hotspot. The TSF Prison Protocol
OBSOLESCENCE	<u>System must be backwards compatible and able to evolve into the future.</u> The world of wireless technology is constantly evolving. A system that is unable to evolve in sync is a complete waste of money. The TSF Prison Protocol System is backward and forward compatible which means it will never be obsolete.
MONITORING	Monitoring must be AUTOMATED and not require additional staff. The TSF system does all monitoring offsite and requires no additional staff nor out-of-pocket expense for the DOC.

TSF KEY FEATURES CURRENTLY BEING CONSIDERED FOR DEVELOPMENT (TSF Engineers Have Confirmed the Following Features Can Be Developed If Industry Participants Deem Support Is Warranted)

Warden Badge Override	Permits the Warden to use his/her phone via a special prison protocol exemption RFID tag name badge. Phone must be within 1 meter of badge.
Auto Snap & Send	During the short period of time between the Guard Alert initialization and the Auto OFF Shutdown actually taking place, the TSF software will direct the device to quickly snap pictures and send them (with location and time identification).
Continuous Guard Alert	Here, the phone bypasses the Auto Off Shutdown feature after the 3rd audible and instead continues the loud guard alert siren until the battery runs dead or is removed.

**Top 11 Performance Measures For Evaluating System Efficacy
For TSF Prison Protocol Technology & Competing Systems
(Voiced By Corrections Personnel and Industry Participants)**

	Performance Measure	Try Safety First Prison Protocol	Jamming Systems	Managed Access Systems	Detection & Location
1.	Is the Technology Solution Legal?	YES	No	With FCC Approval	Yes
2.	Approximate Cost/ Facility?	* FREE * ALL 7,442 Correctional Facilities in the US	\$350K - \$1.2 million Per facility	\$1.2 - \$5 million Per Facility	\$300K - \$1 million Per Facility
3.	System Frequency Containment Issues?	NO	Yes	Yes Urban Environments	No
4.	Effectiveness % to Terminate Service?	< 100% >	N/A	Unknown % (No test and evaluation results)	0% Service NOT Terminated
5.	Obsolescence Issues	NO	N/A	Yes	Yes
6.	Requires On-Site Staff Monitoring?	NO	Yes	Yes	Yes
7.	Are Carrier Agreements Required?	PREFERRED	N/A	Yes	No
8.	Can System Locate Phones?	+ LIMITED + ASSISTANCE	No	No	± Yes ±
9.	Is Carrier Included In Business Model?	YES	N/A	No	No
10.	Does System Dissuade Continued Smuggling?	YES	N/A	No	No
11.	Handsets Require Protocol Inclusion?	◆ YES ◆	N/A	No	No

- * READ ON to learn how the TSF Prison Protocol Business Model outfits every Correctional Facility FREE!
- <> To date, TSF technology has only undergone “Bench Testing.” Actual prison testing is being scheduled.
- + The TrySafetyFirst prison protocol system has an automated Guard Alert function which creates a loud screaming siren prior to disabling and shutting down the phone.
- ± Detection & Locations systems can locate the approximate location of phones ONLY when they are monitored AND the phone is on.
- ◆ Handset protocol inclusion will be viewed by critics as a major hurdle. And while TSF agrees it will be challenging, TSF has designed a specific strategy and migration timeline to mitigate this concern and ultimately prevail (outlined herein). Absolute success and complete compliance will be insured with FCC involvement (See Preamble-Inside Cover & 100% Compliance - Protocol Inclusion, page 11).

OVERVIEW OF COMPETITIVE TECHNOLOGY SOLUTIONS

Jamming	<p>Jamming solutions are illegal. PERIOD! Jamming radio frequency signals is expressly forbidden by <i>The Communications Act of 1934</i>.²</p> <p>Even if jamming solutions were to be approved, they would generate several public safety issues that make them ill-advised. Jamming intentionally creates interference on the frequencies. The interference is difficult to effectively contain and will “bleed over” beyond the correctional facility boundary. When this occurs, legitimate cell phones in the general vicinity are adversely affected.</p> <p>“Jammed” phones may be rendered incapable of initiating/receiving voice calls or text messages, however, other features of the phone continue to function.</p>
Managed Access	<p>Managed Access Systems are very, very expensive. They are expensive to set up and they are expensive to maintain. They require expensive human monitoring and frequent adjustment. MA systems have failed to live up to their hype—i.e., turning a phone into a paper weight (this simply is not true). Even when managed access systems do capture and terminate cell phone transmissions properly, they do not terminate the phone’s other functions including WiFi, camera, audio/video recorder, and word processor.³</p> <p>If the voice capability of a contraband cell phone is terminated, it is a simple matter for an inmate to smuggle-in a new SIM card (the size of a finger nail). A recent Indiana-Purdue University evaluation of the Mississippi State Penitentiary Managed Access System revealed that twelve (12%) percent of all contraband cell phones detected in their study were associated with multiple SIM cards (aka “SIM-swapping”), and had an average “life span” of fifty-eight (58) days in service (i.e., the time span between when a unique cell phone is first detected until it is no longer detected). The independent researchers who evaluated the managed access system in Mississippi concluded that, “For every cell phone confiscated, there are 10 currently available for use.” They further concluded that, a “MAS (Managed Access System) is not a solution; it’s a tool.”⁴</p> <p>The California Department of Corrections and Rehabilitation (CDCR) recently stopped expansion plans of managed access systems. All eighteen facilities where managed access was installed failed to meet expectations and requirements.⁵</p>
Detection & Location	<p>Location & Detection (L&D) systems DO NOT terminate service. L&D solutions facilitate recovery of contraband cell phones so forensic examiners can extract intelligence data. They do not pinpoint the location with adequate accuracy. Extensive human resources are still needed to search a general area to find a phone once detected (the size of the search area is dependent on the number of sensors deployed). They do not disable or prevent any service or functionality of the contraband phone. A graphical user interface provides a facility map indicating the general area of the cell phone. Corrections officers must then be dispatched to search the area for contraband. Inmates have been known to have multiple phones.</p>

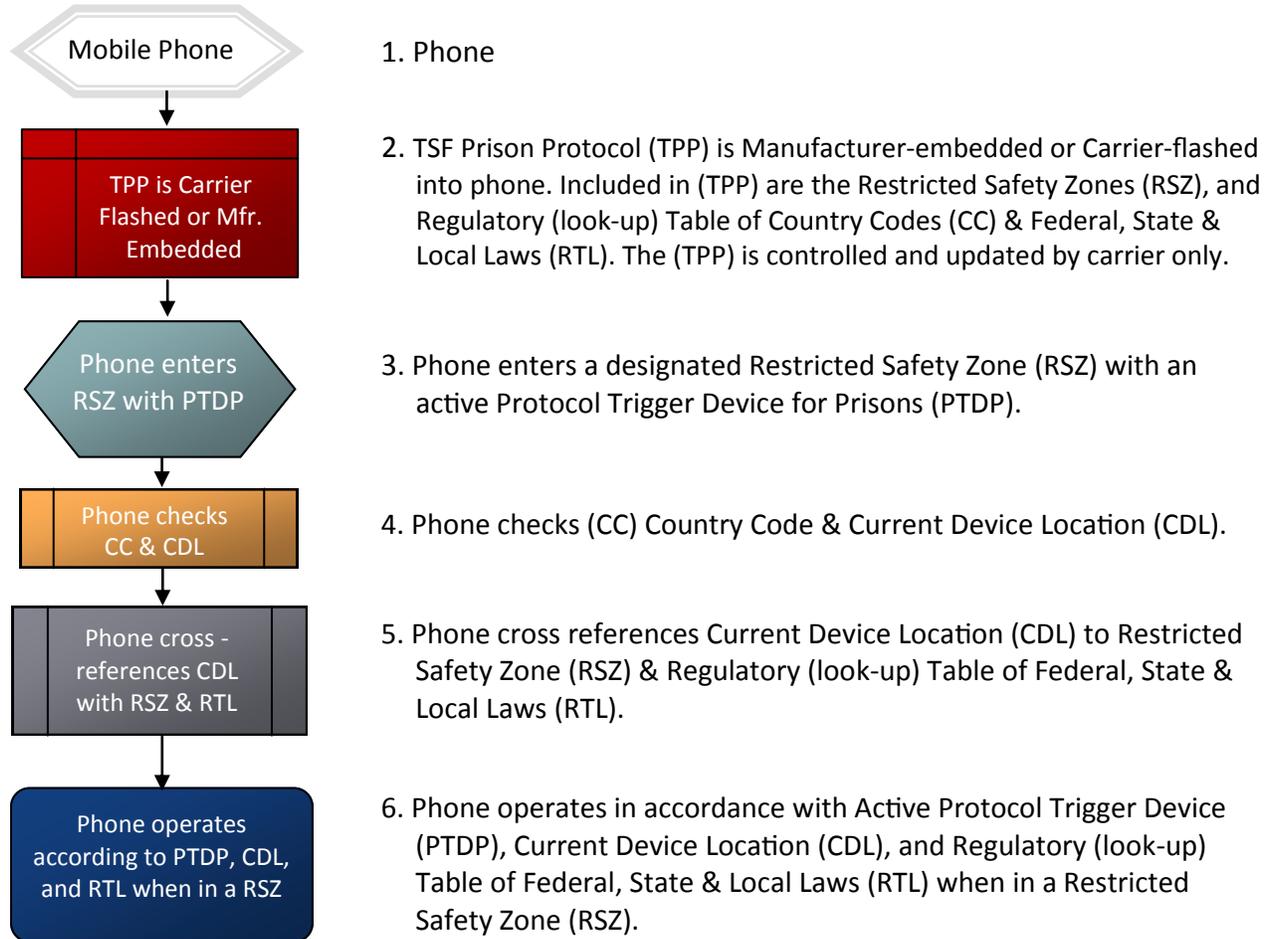
²*The Communications Act of 1934*, 47 U.S.C. § 151 et seq.

³Shaffer, John S., *Cell Phone Forensics in a Correctional Setting Guidebook*, NIJ Award No. 2010-IJ-CX-K003, October 2014.

⁴Grommon, E. and J. Carter, et al., *Assessing the Size of Contraband Cell Phone Use in Prison: Evidence and Implications from a Managed Access System*, NIJ Award No. 2010-IJ-CX-K023, results presented at the ACA Conference, August 2015, Ind., IN.

⁵AllGov.com, *New, but Not Unexpected, Technology Derails State’s Plan to Squelch Prison Cellphones*. Dec. 25, 2015. <http://www.allgov.com/usa/ca/news/top-stories/new-but-not-unexpected-technology-derails-states-plan-to-squelch-prison-cellphones-151225?news=858050>

FLOWCHART



TSF Acronym Key

TSF - Try Safety First, Inc: Inventor of the securitized Prison Protocol technology.

API - Automated Protocol Intelligence: The automated operational procedures of a mobile device functioning according to its current location and the corresponding state laws, regulations, policies and procedures when in a Restricted Safety Zone (RSZ).

TPP - Try Safety First Prison Protocol: The brain of API. Included in TPP are Restricted Safety Zones (RSZ), Restricted Safety Protocols (RSP), and Regulatory (look-up) Table of Federal, State Laws & Local Laws (RTL). The TPP will be controlled and updated by the Carrier only. Once standardized, the TPP will be manufacturer installed.

CC - Country Codes: A coded listing of all countries.

RSZ - Restricted Safety Zone: A specific environment where mobile devices have been deemed to have detrimental effects on society.

RSP - Restricted Safety Protocol: A uniquely designed code of behavior for operation within a specified Restricted Safety Zone environment.

RTL - Regulatory (look-up) Table of Federal, State & Local Laws for Mobile Devices: Comprehensive table of mobile device laws, regulations, rules, policies and procedures. (controlled by carrier only)

PTDP - Protocol Trigger Device for Prisons: A unique (1-15m limited range) transmitter capable of broadcasting a Restricted Safety Zone environment specific trigger signal.

APTD - Active Protocol Trigger Device: A protocol trigger device that is turned on and is broadcasting a Restricted Safety Zone environment trigger signal.

CDL - Current Device Location: The current location address (country, city, state and zip) of a mobile device receiving a signal from an APTD.

ADDITIONAL DETAIL - How It Works

The **TPP** (see below) search and response safety function is added to the existing firmware of all phones. Upon initial boot-up and continuing with each algorithmic base station scan, the **TPP** searches for the **PTDP** Beacon. Specific device recognition of a triggered protocol signal will override the normal operational functionality of the device and force the device to shut down.

More specifically, the inventive technology as a whole and described herein is called Automated Protocol Intelligence (API). The system comprises two distinct parts, one part hardware and one part software - both necessary for proper implementation. The parts will be defined and explained herein as the Try Safety First Prison Protocol (TPP) and the Protocol Trigger Device for Prisons (PTDP):

Try Safety First Prison Protocol (TPP) – The new search and response safety algorithm software protocol to be embedded into the firmware of the Mobile Device.

Protocol Trigger Device for Prisons (PTDP) - simulates a beacon - The precision range hardware is strategically installed in specific areas in the correctional facility known as Restricted Safety Zones where mobile device regulation is to be automated. Upon PTDP activation, the Device acts like a beacon inside the specific range area.

Normal Cell Phone Operation: When a cell phone is first powered up, an algorithm inside the phone scans for the proper base station tower over which it should communicate. Once the base station is selected, packets of information containing special codes are sent back and forth to a Mobile Telephone Switching Office (MTSO). This exchange is completed over a special frequency only used for call set-up and channel changing. The special frequency is called the control channel. The control channel is the initial frequency for a wireless device to register operability. Normal talk and data transfer are not completed across the Control Channel. Once registration is complete, the phone will continue to scan in timed increments (usually 20 or 30 seconds) to be sure it is operating across the best or preferred network using the best or preferred base station tower.

New Cell Phone Operation With Try Safety First Prison Protocol (TPP): *When a cell phone is first powered up, the Try Safety First algorithm will scan first for a (PTDP) Protocol Trigger Device for Prisons. If an active Protocol Trigger Device is found, the mobile device will identify its exact geographical location and then cross reference the device and apply proper operation according to the legislative laws, regulations and policies as set forth by governing bodies and or authoritative policy in the country where the device is operating. If no active Protocol Trigger Device is found, the phone operates according normal operating procedures. As the phone continues to scan (usually every 20 to 30 seconds) to be sure it is operating across the best or preferred network using the best or preferred base station tower, the scan will always include a search for an active Protocol Trigger Device for Prisons. All scans are performed across control channel frequencies. This is important as this will make certain any necessary operational change will take place in the quickest manner possible.*

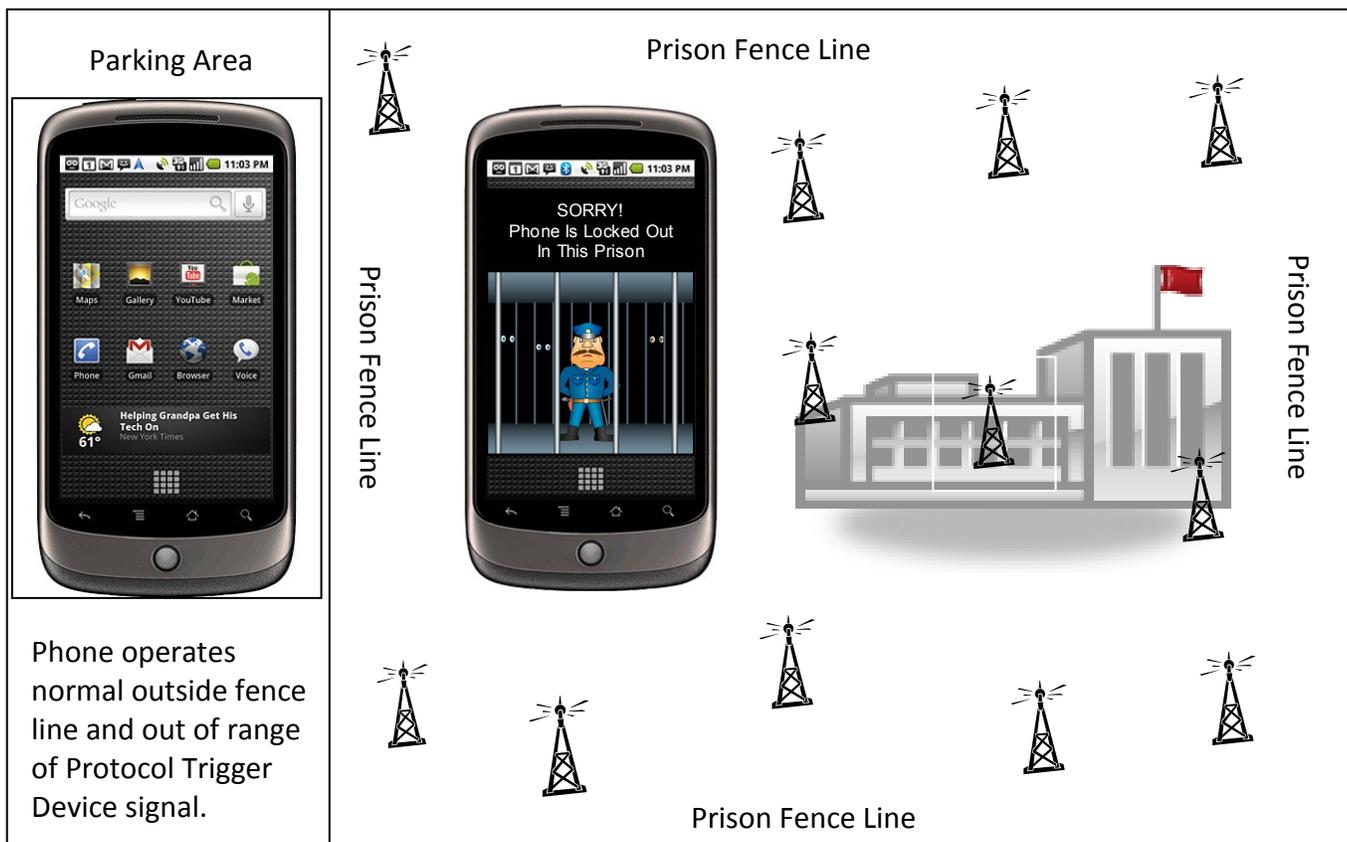
The TSF Prison Protocol technology does NOT track, it does NOT listen, it does NOT record, it simply turns itself off when in the restricted safety zones of a prison facility.

PTDP - PROTOCOL TRIGGER DEVICE FOR PRISONS

A PTDP is a unique precision range transmitter/beacon (1—15 M). The TSF engineered device acts similar to a miniature base station tower such that it is capable of broadcasting a securitized Prison Protocol Code within a specific location area identity (LAI). **The Prison Protocol Code is broadcast across the control channel frequency.** This is important as this is the frequency used to set-up and establish service and determine the phone is in good standing prior to connecting to the normal talk and text frequencies. The power at which the device will operate is much lower than a traditional tower signal as there is no need for back and forth frequency communication. The phone simply needs to receive a signal from an active PTDP during it's algorithmic tower search to understand it is in a Restricted Safety Zone prison area and must shut down.

Prison Example

TSF Prison Protocol Enabled Phones Understand Restricted Safety Zones



 Limited range Protocol Trigger Devices for Prisons (PTDPs) are strategically placed inside the prison fences and buildings to broadcast the prison protocol trigger signal. All phones housing the TSF Prison Protocol software will commence shutting down once inside prison fence line and in range of the broadcast trigger signal (PTDP's can be programmed 1 - 15 m).

**100% EFFECTIVE
TSF TECHNOLOGY REQUIRES FCC ASSISTANCE**

For the Try Safety First Prison Protocol Technology to be 100% effective, 100% compliance must be achieved. The only way this will occur is for The FCC to establish & indoctrinate a new securitized prison protocol safety standard for the wireless industry. In doing such, the FCC will issue a new regulation by which ALL Carriers and Manufacturers are bound to comply. The new regulation will establish a new rule with two independent parts. One part will apply to the Carriers and the other part will apply to the Device Manufacturers. The FCC will also establish a migration period with a firm deadline.

NEW RULE: A phone is not permitted to access any network unless the phone is safety protocol verified by the carrier. Whenever the phone boots up or attempts to access any carrier network, the network must system check the phone to make sure it is protocol enabled. This is to be completed by the carrier whose network the phone is trying to access. Explained in further detail: Currently, when a phone boots up or attempts to access a carrier network, the carrier system checks the phone to make sure it is in good standing (i.e., has the bill been paid – if the bill has not been paid the phone is not considered to be in good standing and is unable to access the network – except when dialing 911). Under the new rule, for a phone to be considered to be in good standing it must also satisfy the safety protocol verification requirement or carrier access will be denied.

Part 1 - Carrier Frequency Agreement – A new provision will be added to the Carrier Agreement. **The provision to be included in the carrier agreement will state that no phone is permitted access to any carrier network that isn't safety protocol enabled.** (See 100% COMPLIANCE—PROTOCOL INCLUSION (page 11) to learn how phones become prison protocol enabled via the Carriers).

Part 2 - Pertains to manufacturers, importers and distributors – A **new component requirement** will be added to the product certification process for all wireless telecommunication devices. The requirement will state **no wireless telecommunication device will receive product certification approval unless the device is firmware embedded with the securitized safety protocol for prisons.** (See 100% COMPLIANCE—PROTOCOL INCLUSION (page 11) to learn how phones become prison protocol enabled via the Manufacturers).

100% COMPLIANCE—PROTOCOL INCLUSION

How Phones Become Protocol Enabled

In order for the Try Safety First Prison Protocol technology to be 100% effective, we first must achieve 100% compliance. This means ALL phones in the U.S.A. must be prison protocol enabled. This will be achieved in the following manner:

The FCC passes a new regulation. The regulation will contain very specific language establishing a firm future date by which all mobile devices must be prison protocol enabled. After said date, devices that are not prison protocol enabled will be refused access to all carrier networks. For purposes herein the period between establishment of the regulation and the actual date on which all devices **MUST** be protocol enabled will be referred to as the migration period (more on this to follow).

During the migration period, all mobile devices will become protocol enabled in 1 of 4 ways as follows:

1. The phone will come prison protocol loaded from the manufacturer. (preferred method and eventual end all be all)
2. The phone will become protocol enabled following a system update via USB hardwire to the manufacturer website.
3. The phone will receive a system update from the Carrier using **FOTA – Firmware-Over-The-Air**. (Quickest method) (The Carrier will perform the system update only after receiving an updated source code containing our protocol from the Manufacturer - more on this later).
4. TSF will set up a website linked to both manufacturers and carriers. On phones that do not properly receive the FOTA update (and there will be some), TSF engineers will provide customer service and support to guide Carrier customers thru a hardwire download. In the event a customer's phone is so outdated (instances might include old analog phones where the manufacturer is out of business and there is no source code available) – we have to be prepared to offer the customer either a used replacement phone or encourage the customer to upgrade their device through their carrier.

We know we are going to incur this migration phase – it's the only way to achieve 100% compliance. Anything less will leave open gaps and points of failure.

100% CONTROL OF PTDPs

Top security measures will be taken to insure **ALL** TSF protocol trigger devices for prisons are known and accounted for at all times. A specific manufacturing and distribution control center shall be established. All devices will be security coded and in need of specific procurement requisition for release from the center. Old non-working devices must be returned to the distribution center.

2 YEAR PROTOCOL INCLUSION TIMELINE—Example

(To Be Established by the FCC)

- 1-1-2018: FCC issues new regulation including timelines.
- 3-31-2018: Carrier supplies to TSF complete contact information for all phone manufacturers currently operating on Carrier's network.
- 4-30-2018: TSF contacts cell phone manufacturers and delivers Software Development Kit (SDK) containing securitized safety protocol for prisons.
- 1-1-2019: Existing Phones: Manufacturers will write a source code update and supply the Carrier with the update for FOTA (see Below).
- 3-31-2019: New Phones: All new phones manufactured, imported and/or distributed in the U.S. must be Safety Protocol Enabled. Phones that are not will NOT pass the FCC Product Certification Process and will not be able to access any carrier network.
- 3-31-2019: Manufacturer/TSF Special Website Link – Manufacturers will also be required to either (1) include a website link where existing customers can connect via wired line from their computer to accept a system update for phones unable to accept FOTA (see below), or (2) provide TSF the updated source code and TSF engineers will offer customer support for the wired update.
- 4-30-2019: Carrier - FOTA – Firmware-Over-The-Air: This is the process where the carrier will perform a system update to all phones on their network. Somewhere between 80% - 90% of phones will be able to be updated over-the-air in this fashion. Once the update is complete, the carrier will perform a system check and provide TSF a complete listing of all phones and manufacturers that were not able to accept the system update. The carrier will send an automated response to the customer stating the security update was not completed properly and to contact the carrier. This will be a Carrier/Customer choice to either upgrade to a newer phone or in cases where the customer elects not to upgrade, (we will have a specific contact number set up to transfer calls where we will discuss all options with the customer – either do hardline inclusion or get a new or used phone that can be protocol enabled).
- 1-1-2020: Carriers must system verify the phone is in good standing (security protocol enabled) prior to providing network access.

COST TO OUTFIT ALL CORRECTIONAL FACILITIES

**102 Federal Penitentiaries ♦ 1719 State Prisons ♦ 2259 Juvenile Detention Centers
3283 Local Jails ♦ 79 Indian Reservation Detention Centers**

Try Safety First has developed a unique business model which: 1) generates funds to outfit ALL correctional facilities and 2) creates a new revenue stream for the Carriers for their participation. This allows ALL correctional facilities to fully participate. It is imperative that all correctional facilities are able to have the contraband cell phone problem corrected. Many states simply do not have the budget requirements to even consider spending large amounts of money to tackle this problem. It is also important for the Carriers to be compensated fairly for their necessary contribution to correct the problem.

For the past several years there are people on both sides of the argument regarding who should foot the bill to cover the necessary expenditures to correct the problem of contraband cell phones. Wasting time arguing who is at fault and who should pay is of no value in these life experiences. The bottom line is this: There is a major problem and it is not going away on its own. The longer it is left unattended, the more difficult it becomes to solve and the more innocent people get harmed. This is an industry problem and therefore the consumers of wireless technologies should bear the expense. The business model TSF has developed directly supports this theory.

Bottom Line: The cost will be absorbed by the users who subscribe to wireless services. As things currently stand, the estimate to properly outfit the average prison facility is \$250,000. The ongoing cost estimate for off-site equipment monitoring and on-site yearly maintenance is \$24,000 per year per facility. The total expenditure and the time required to completely outfit all 7,442 institutions will be amortized over a 7 year period. Using industry figures and basing the calculations on the total number of active wireless devices:

Added Monthly Cost Per Device = 17¢

IMPORTANT NOTE: We are constantly sharpening our pencil and looking for ways to reduce this cost. Original estimates to cover all expenditures were 49¢ per month. This was unacceptable to the Carriers. Learning this, we reconfigured and re-amortized timelines to get it down to 17¢. We are still working on this. It is important to note it may be possible a lower fee is accepted for a defined period of time, but it should be understood that a new negotiated fee may need to evolve every few years based on realized costs. **Additionally, TSF is currently speaking to DOCs & Inmate Phone System Providers to look for ways to shave installation costs. Results will provided in the near future.**

It should also be noted the 17¢ monthly added cost includes a reasonable administrative fee to be paid to the Carriers for their participation.

For a more detailed analysis, if you are an industry participant and are interested in working with us to solve this problem, please contact:

John Fischer
770-652-4517
john.fischer@trysafetyfirst.com

PILOT TEST PROJECTIONS

Try Safety First anticipates undergoing two separate pilot tests in the coming months. The first test will be in an empty prison facility. This will enable engineers and examiners to freely move about in and out of multiple areas. This will advance greater knowledge and know how should system modifications and or adjustments need to be completed. The second test will be an operational field test and evaluation (T&E) conducted in an occupied correctional facility."

PILOT TEST PROCEDURES:

- A. We will enter the prison and strategically place our security beacons throughout the prison.
- B. Several test and evaluation (T&E) teams will be handed one of our test phones as they enter the prison (approximately 20 phones).
- C. They will be instructed to walk throughout the prison and make phone calls, send texts and emails, get on facebook, etc. at their leisure for approximately 5 minutes.
- D. We will then proceed to upload our protocol into all 20 test phones: (using 3 methods IF POSSIBLE)
 - (i) The 1st and preferred method of upload will be wireless also known as FOTA – firmware-over-the-air. We are hoping to gain FCC approval and Carrier compliance to assist us. If we do not get this assistance, our engineers will attempt to conduct this on their own FOTA build.
 - (ii) The second method will be to use non-protocol enabled phones. They will be tested with the beacons on to prove they are not protocol enabled. The beacons will then be returned to the OFF position. The phones will then be hooked up to a computer inside the facility and the protocol will be uploaded via hardwire.
 - (iii) The third method will be to have the test phones already enabled prior to handing them out.
- E. Once all T&E phones are protocol enabled we will instruct the participants to continue using them.
- F. We will now activate the beacons and watch the phones become disabled.
- G. Instruction will be given to the participants to continue walking throughout the prison facility while attempting to make calls, send texts, send emails, etc.
- H. We will then instruct some of the participants to venture outside the prison gates to prove that once the phone is no longer within range of the beacon, it will resume normal operation.
- I. After a predetermined elapsed period of time, we will deactivate the security beacons inside the prison.
- J. The participants will be asked to wait a few minutes, then told to make calls to show all phones work normally once they are outside the range of the protocol beacon.

End of pilot test

Peer Review Analysis by Corrections Industry Expert John S. Shaffer, PhD



Credentials: John S. Shaffer earned a Ph.D. and an MPA from the University of Pittsburgh and a BA from Westminster College. He served 31 years with the Pennsylvania Department of Corrections, retiring from his position as the Executive Deputy Secretary in December 2007. Since 2008, he has served as an expert consultant for public and private sector clients and non-profit agencies in the US and UK. Dr. Shaffer has authored and co-authored multiple industry papers including *Fostering Innovation in Community and Institutional Corrections - Identifying High-Priority Technology and Other Needs for the U.S. Corrections Sector*; *Cell Phone Forensics In A Correctional Setting: Guidebook* written for the USDOJ; and he was the co-Principal Investigator and author of the NIJ classified report, *Test and Evaluation of Hand-Held Cell Phone Detection Devices*.

Try Safety First, Inc. (TSF) has developed a new, patented, method for terminating contraband cell phones in the corrections environment. This emergent technology solution to the contraband cell phone problem is unique, promising, and worthy of further test and evaluation.

Unlike jamming solutions, the TSF protocol does not indiscriminately terminate cell phones outside of the Restricted Safety Zone (i.e., correctional facility), and it allows for 911 calls in an emergency. It only terminates cell phones that have been designated contraband by statute or regulation.

Unlike managed access systems (MAS) that only terminate voice and text messaging services and provide no location information, the TSF solution will also terminate all other cell phone functionality (i.e., photos, videos, word processing, Bluetooth, and Wi-Fi hot spots). Current MAS systems have proven to be high maintenance and less than 100% reliable. TSF's wireless beacon network reduces initial installation costs and allows for centralized off-site monitoring. TSF maintenance would consist of periodic battery and occasional sensor replacement.

Unlike detection and location solutions that do not terminate cell phone service and only provide a broad search target area, the TSF technology does not require staff to monitor the system and it does not require the deployment of search teams to look for cell phones.

Bench testing has demonstrated that the TSF solution will cause a security-protocol-enabled cell phone in proximity (1-15 meters) of a TSF beacon to emit a piercing audible alarm that may allow staff to detect it. It may also be able to photograph the cell phone user and his environs, record the GPS fix, and email both to security investigation staff during the shut-down phase. This will enable investigatory staff to identify and question the individual in possession of the contraband cell phone. If the phone is recovered, it may have some security intelligence data worth investigating. Bench testing has demonstrated that when the TSF Protocol terminates a cell phone, it ceases to function in any capacity. The cell phone is, in fact, rendered useless.

The business model that enables funding for national implementation over a multi-year migration period is grounded in the existing public safety language of current carrier agreements. Carriers have an existing mechanism (the Regulatory Cost Recovery Charge) that will allow them to recover their investment in public safety and install the technology at every correctional facility in the US. The cost to the individual cell phone user would be nominal.

The next step in the evolution of the TSF solution is to conduct operational testing. A proof-of-concept installation at an unoccupied correctional facility, with subsequent testing in a functional facility would be advisable. Assuming that the operational testing is successful, what is it going to take to make the TSF solution a reality? It will require the FCC to mandate that the TSF security protocol must be installed on all existing cell phones operating in the US. It will require the cooperation of all cell phone carriers to push-out the required firmware to their user base. And, it will require all cell phone manufacturers to install the TSF security protocol on all new cell phones during production. These are not insignificant challenges.

John S. Shaffer, Ph.D.