BINGHAM

Danielle Burt
danielle.burt@bingham.com

July 30, 2013

VIA ELECTRONIC FILING

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

Re: WC Docket No. 12-375 - Rates for Interstate Inmate Calling Services
Notice of Ex Parte Presentation

Dear Ms. Dortch:

On July 29, 2013, Jay L. Gainsboro, President and Founder of JLG Technologies, LLC, Mike Kester (by phone) of JLG Technologies, LLC, Alex Fox, Practioneer and Consultant, Don Wood (by phone) of Wood and Wood Associates, and the undersigned counsel for JLG Technologies, LLC, met with the following representatives of the Wireline Competition Bureau: Randolph Clarke, Deputy Division Chief of the Pricing Policy Division, Douglas Galbi, and Gregory Haledjian.

During the meeting, Mr. Gainsboro and Mr. Fox commended the Commission for taking action to address interstate rates for inmate telephone calls. They presented information about public safety issues from the use of inmate calling services and emphasized the continuing need for security features in the inmate telephone system. They distributed two hand-outs which are attached as Attachments A and B.

Mr. Gainsboro responded to questions about data presented in the JLG Technologies, LLC white paper, a redacted copy of which is attached as Attachment C. Specifically, he explained that the voice recognition biometric technology used by his company can verify when third parties join a call but cannot specifically identify third parties since third parties are not required to enroll in security programs like inmates. His company has been able to use its technology to determine that one out of every 14 inmate calls is made covertly (*e.g.*, inmates try to hide their identities through pin sharing, pin stealing, and/or three-way calls). In a recent analysis of phone calls conducted by JLG Technologies, JLG's biometric based 3-way call detection technology detected at least one 3-way call on 3.8% of the suspicious calls that its systems uncovered. Mr. Gainsboro described the cost to inmate calling service (ICS) providers for JLG Technologies, LLC's security technology is $0.02 per minute. The most common price charged to rate payers by ICS providers when JLG Technologies Products are provided to correctional facilities is $0.25 per call. These fees are also usually non commissionable to the correctional facility. He noted that costs for security technology for non-traditional voice services (*e.g.*, Voice over Internet Protocol) tend to be more expensive, particularly because conventional means of determining when three-way calls are initiated do not apply.

Mr. Gainsboro and Mr. Fox recommended that any new rate policy adopted by the Commission for inmate telephone calls account for the cost of meaningful ICS security

Boston
Hartford
Hong Kong
London
Los Angeles
New York
Orange County
San Francisco
Santa Monica
Silicon Valley
Tokyo
Washington

Bingham McCutchen LLP
2020 K Street NW
Washington, DC
20006-1806

T 202.373.6000
F 202.373.6001
bingham.com

technology. The cost of meaningful ICS security technology may vary for different correctional facilities and agencies, and a "one-size fits all" policy may have unintended negative consequences. Mr. Gainsboro suggested the Commission might consider allocating a per-minute cost for telephone security in any new rate structure as long as telephone security measures are being deployed or updated as part of ICS. Mr. Gainsboro and Mr. Fox also suggested the Commission might coordinate with the National Institute of Justice or another entity knowledgeable about security systems regarding the value and costs of telephone security technology.

Pursuant to Section 1.1206 of the Commission's rules, a copy of this letter has been filed via ECFS and sent by email to each of the Commission staff members who participated in the meeting. If you have any questions, please do not hesitate to contact the undersigned.

Very truly yours,

/s/ electronically signed

Danielle Burt

cc (by e-mail): Randolph Clarke
Douglas Galbi
Gregory Haledjian

ATTACHMENT A

INMATE PHONE CALLS AND THE PUBLIC SAFETY DETERMINING THE PROPER BALANCE

Jay L. Gainsboro
President & Founder, JLG Technologies, LLC
Alex Fox –Practioneer, Consultant

July 29, 2013

Meeting Objectives

- To Provide The FCC with Inmate Calling Public Safety Related Information So That The Commission Can Make An Informed Decision About Whether Specialized Public Safety Related Technology Should Be A Part Of Its New Rate Plan For Inmate Phone Calling.

Public Safety Threat

- Many inmates continue to commit crime while incarcerated
- Inmates utilize the telephone to communicate with individuals in the community to conspire and carry out serious criminal activities
  - Murder of victims, witnesses, and others
  - Organized Crime & Violence
  - Drug-Related Crimes
  - Sexual Assault
  - Fraud, Theft and Other Money-Related Crimes
- Inmates victimize vulnerable populations
  - Crime victims
  - Witnesses and Informants
  - Judges, District Attorneys, and Jurors
  - Law enforcement and correctional personnel
  - Fellow inmates
  - Family members of other inmates
  - Innocent people in the community
- Gangs are rampant in corrections and pose one of the most serious security threats in corrections and to the public
  - Inmate gang members are known to commit especially heinous crimes in concert with gang members on the street

Prison Environment and Security

- Prisons are highly dangerous and vulnerable environments that require specially designed items to ensure safety and security
- All products and items in prisons must be specially constructed to ensure they are not tampered with or misused as a weapon or to commit crime
- Like all products used in prison, extra security features must be embedded in the inmate telephone system to prevent inmates from circumventing its intended use

Technology and Telephone Security

- Inmates utilize sophisticated techniques to breach telephone security to communicate with co-conspirators and avoid detection
- Telephone system technology is a critical tool to combat continued criminal activity by inmates
- Security features allow correctional staff to identify perpetrators, preempt crime, and prosecute crime
- Without advanced telephone security features it is nearly impossible for staff to adequately identify planned or executed crimes and protect the public from harm

ICS Security Technology

- Technology Provides The Only Viable Defense Against Inmate's Use Of The ICS For Criminal Activities
- 1 out of Every 14 Calls Inmates Make Are Made Covertly
- Technology:
  - Protects Inmates & Their Family's Funds From Theft
  - Greatly Reduces The Correctional Agency Labor Costs Associated With Keeping The Public Safe From Inmate Criminal Calls

What Does This Type Of Technology Cost?

- JLG Technologies Charges ICS providers ~$.02/minute
- ICS Providers Add Their Own Costs For The Technology To This Rate

Who Should Pay For Inmate Telephone Security?

- The Impression Conveyed By NASUCA Is That Every Inmate Phone Call Is One Step Closer To Reducing The Inmate's Likelihood Of Committing Another Crime.
- The Reality Is: In 1 Out Of Every 14 Inmate Calls Placed In The U.S. Inmates Attempt To Circumvent The Security Of ICS Systems.
- Inmates And Their Friends and Families Are The Ones Using The ICS To Conduct Illicit Activities.
- We Believe Users Of The ICS Should Be Bearing The Cost For Inmate Telephone Security.
- Countless Business Examples – Cell Phone Providers, Wireline Providers, Banks, Cable TV Providers Include The Cost Of Security In Their Rates

Summary

- ICS Security Technology Is The Only Affordable Way To Assure That ICS Is Safe For Inmates & The Public
- The Costs For ICS Should Be Borne By The Users Of The ICS
- The Industry Currently Has A Means To Fund 3rd Party Inmate Calling Security Technology Through A Surcharge.
- We Are Concerned That The FCC's New Rate Policy Could Have Unintended Consequences By Eliminating An Existing Security System Which Could Result In Loss Of Life And Other Harmful Outcomes.

Alex Fox Correctional Tech, Ops Expert

- 30+ years in correctional ops, tech and senior warden
- Founder, NTPAC
  - *Northeast Technology Product and Assessment Committee*
- Co-founder, ADF Consulting
  - *International corrections technology company*
- Co-author, *Correctional News* column *Fox TechWatch*
- Chair, ACA Tech Applications, Intelligence Committees
  - BOD, Law enforcement technology organizations
  - Expert, DOE vulnerability assessments

Sandia National Laboratories

Massachusetts Department of Correction

Department of Defense United States of America

Correctional design+construction+operations

ACA

Jay Gainsboro President & Founder

- Key Evidence For The Oklahoma City Bombing Trial – Timothy McVeigh
- 30+ years in telecommunications; 25+ in corrections
- Founded 5 successful leading-edge, high-tech companies
- More than 100 patents and patent applications
- Founded JLG Technologies in 2005
- Launched the *Investigator Pro Inmate Phone Security System* in 2007
  - *Now monitoring 80k+ inmates in over 150 facilities in 23 states*
- B.A., Management Sciences, Worcester Polytechnic Institute
- Jay L. Gainsboro email: jay@jlgtech.com – Phone: 508-788-1787

ATTACHMENT B

Threat to the Public Posed by Inmates Who Breach the Telephone System to Commit Crime

- Ensuring public safety and security is the mission and responsibility of corrections. It is imperative that a balanced approach is taken to providing consistent and reasonable inmate telephone service rates and commissions while at the same time affording correctional agencies the ability to use and obtain the most advanced security systems for their phones to mitigate and preempt criminal activity. Reducing rates too far opens the door to re-victimization and possible loss of life and that is far too great a cost to pay.

- When it comes to the use and misuse of the inmate telephone, there are many possible victims to consider. It is acknowledged that excessive rates can cause a financial hardship for family members who have not committed a crime but rightfully want to maintain communication with their loved one. However, it is a harsh reality that inmates can and do breach the security of the telephone system - and when they do they create additional victims.
    - Many inmates are incarcerated for crimes against wives, girlfriends, children and other family members. Many have restraining orders against them. They become victims yet again when inmates use the phone to harass, threaten, and sometimes carry out plans to have them killed.
    - Inmates commit crimes against the family members of other inmates
    - Inmates engage in victim and witness intimidation and murder
    - Inmates victimize and sexually assault other inmates in retaliation
    - Inmates create multiple victims of their organized crime, drug trafficking, and fraud operations
    - Inmates endanger the lives of staff, other public officials, and the general public

- It is well known in the correctional community that organized gangs pose the most serious security threat in corrections and to the public. The FBI estimates that there are approximately 1.4 million active street, prison, and outlaw motorcycle gang members comprising more than 33,000 gangs in the United States. There are approximately 230,000 gang members incarcerated in federal and state prisons alone nationwide – and that staggering number does not even include county facilities and jails. At any given time there are members of the same gang in prison and on the street. Gangs operate through orders given by gang leaders to gang members to commit crimes. This criminal enterprise structure is unbroken regardless of whether or not these individuals are incarcerated. Gangs are known to commit some of the most violent and vicious crimes. The most heavily relied on means of communication to conspire is the use of the inmate telephone. Gang members are

Alex Fox – Dorothy Fox - 4915 Bear Way Prescott AZ 86301 – (508) 488-0808 – techfox@cableone.net

known to utilize the most sophisticated methods to circumvent the telephone security systems in order to avoid detection.

- Prisons are dangerous and highly vulnerable environments and as such security is number one. Almost anything an inmate has access to can be used as a weapon. Even seemingly innocuous items intended to do good are often used to do harm. As a result, they are reengineered specifically for prisons to ensure that they are not used as weapons or with mal-intent. For example, blankets are constructed with break-away threads to ensure they cannot be fashioned into a rope that could be used for escape, suicide, or homicide. Toothbrushes are constructed with special polymers that cannot be melted or sharpened into weapons. Razors are intentionally etched by lasers so that if they are tampered with they will fragment into hundreds of pieces, rendering them impossible to craft into a weapon. Even broom handles are designed with lightweight material that prevents them from being used as weapons. While all these items have the potential to endanger staff and other inmates within the prison, the inmate telephone poses an additional danger as it can also be used to reach out and harm innocent people in the community. Like all other products used in corrections, the inmate telephone system must include imbedded security features to prevent or minimize its use as a weapon. And like all other products used in corrections these specially engineered systems and services come at a cost that exceeds the cost of the same item for the general public.

- The inmate telephone system is one of the most critical tools in corrections to combat continued criminal activity and threats to the public. Because inmates are incarcerated, in most cases they can only orchestrate and carry out these crimes with the help of individuals in the community. They utilize all available means of communication including the inmate telephone, mail, and visits to orchestrate plans with co-conspirators in the community. Telephone contact is the most widely used form of communication to engage in these dangerous activities. They continuously use sophisticated methods to circumvent telephone security measures to avoid detection. In order to detect, preempt, and prosecute crimes corrections must identify the inmates engaged in these activities as well as the actual plans and incidents. Given the thousands of calls that occur on a daily basis in many facilities it is nearly impossible for staff to identify the perpetrators and incidents in time to prevent them. It is also extremely difficult to investigate and prosecute crimes that have occurred. Monitoring the telephone system is often the most powerful tool and the first thing staff go to when there is an escape, homicide, assault against staff or another inmate, gang related incident, victim or witness intimidation, or other serious crime. In this day and age technology is the standard tool in society that people rely on. It is imperative that the technology tools staff need to protect innocent life not be taken away from them or for new advances in technology to become prohibitive to obtain in the future. Technology has been and will continue to be one of the most valuable and often the only tool at staff's disposal to stop inmates from breaching traditional telephone systems – which is quite easy for them to do

Alex Fox – Dorothy Fox - 4915 Bear Way Prescott AZ 86301 – (508) 488-0808 – techfox@cableone.net

when imbedded security systems are absent or weak. In order for staff to combat this very serious problem their hands must not be tied.

- Failure to adequately secure inmate telephone systems to the greatest extent possible has unintended but dire consequences. While there are many stakeholders in the rate and commissions debate with valid concerns, the number one priority and highest degree of responsibility must be to the most vulnerable victims of all. The threat of inmates using telephone communication to conspire with others in the community to commit murder and other heinous crimes is very real. These potential victims may not know they are at risk and cannot speak on their own behalf. The *fact* is that serious crimes committed by incarcerated individuals have and do occur. They will likely increase if correctional agencies are further fiscally constrained in their ability to maintain the best telephone security systems possible. It is essential that a responsible balance be achieved between reasonable rates and commissions alongside with safeguarding those systems and protecting the public.

Alex Fox – Dorothy Fox - 4915 Bear Way Prescott AZ 86301 – (508) 488-0808 – techfox@cableone.net

ATTACHMENT C

Determining
The Optimal Balance:

Balancing the Cost of Inmate Phone Rates While Protecting Vulnerable Populations – Victims, Witnesses, Jurors, Public Servants, Jail/Prison Staff and Inmates – as well as the General Public

A White Paper in response to United States Federal Communications Commission's Notice of Proposed Rulemaking, in the Matter of Rates for Interstate Calling Services, WC Docket No. 12-375

By Jonathan Klein
Journalist, Systems Designer & Inventor
in Collaboration with JLG Technologies, LLC

July 2013

Executive Summary

Inmate Calling Service (ICS) systems, in use in jails and prisons throughout the U.S., are a dual-edged sword.

On the one hand, ICS telephones have been widely shown to help lower recidivism rates for the inmates that use them — which, in turn, enhances future public safety. On the other hand, these same phones have been shown to be the *Number One communication security threat* to jails and prisons in the U.S. As conventional security systems designed to safeguard the ICS are routinely defeated by inmates, they have demonstrated only limited effectiveness. As a result, inmates in the U.S. continue to commit crimes using the ICS in considerable volume — recently discovered to involve nearly 7% of all ICS calls (as will be shown), if not more — even as they serve time.

Documented cases of such crimes using the ICS include threatening, intimidating, blackmailing and murdering crime victims as well as jurors, witnesses, informants, public servants and others — in addition to a broad array of other criminal activities. As will be shown in this white paper, these particularly vulnerable populations — members of the general public whose lives have become entangled with inmates, and thus brought to inmates' attention, have been one of the main targets of criminal activities perpetrated by inmates while they are incarcerated — using the inmate phone systems provided by the agencies that hold them — to carry out crimes against these individuals.

The very existence of the ICS, therefore, both helps society and poses unique risks to it. These questions of public safety — and especially threats to victims and these other vulnerable populations — are a critical, yet potentially under-discussed, aspect of the case before the FCC. How *might* one go about redesigning a system to mandate lower rates for inmate phone services, while at the same time making sure that the safety of victims, others at particular risk, as well as the public at large, stay protected?

When ICS phones were first introduced in the U.S., the policy was simple: Inmates made very few calls, and every second of every call made by inmates was listened to by correctional staff. This comprehensive monitoring helped contain what has, with increasing inmate populations, tightened correctional budgets and greatly expanded access to inmate phones, become a pervasive threat: Inmates who use the ICS to commit crimes. Manual monitoring of such calls long ago grew unfeasible and impractical, and persistent efforts to replace this approach with both policy changes and security systems have met with results that, at best, might be deemed "mixed." And, as we shall see, the effects of the crimes perpetrated by incarcerated inmates manifest far beyond the walls that hold them — as well as within those walls, to the deleterious effect of another vulnerable population: other inmates.

In the last eight years, a new breed of sophisticated security technology has been developed for the ICS that holds the promise of repairing this security breach. The technology, known as ACTFIRST (short for *Automated, Comprehensive Technology For Identity Resolution Security of Telephones*) monitors every second of every inmate call, bringing the most suspicious calls to the attention of correctional staff. Deployed in 150 jails and prisons in 24 states starting in 2007, ACTFIRST systems have demonstrated effectiveness (as well as *cost*-effectiveness) at finding offending inmates, containing criminal activities that involve the ICS, and protecting vulnerable populations as well as the general public.

This white paper is written in collaboration with JLG Technologies — an independent, Massachusetts-based company founded in 2005 that developed the first ACTFIRST-level system for the ICS. The company offers this technology to ICS providers as well as jails and prisons in the U.S. as an independent, per-minute or per call service that links to the ICS and provides its information to the agency in which it is installed. In the process of developing the ACTFIRST standard, the company has built considerable expertise in the areas of ICS systems, how they work, the risks they pose, and ways to effectively address those risks — as well as the costs associated with them.

Since this expertise is not widely available to the general public, we believe it to be our duty, as well as a matter of public service, to try to help inform these under-served aspects of the case before the FCC. In order to support the FCC's goal of achieving a balanced, evidence-based and effective approach to mandating more affordable rates for inmate calls, we respectfully submit this white paper for the FCC's review.

For the record, we wish to express our position about this case up front. To us, the facts and challenges facing the FCC are clear: Inmates, their families and others that pay for inmate calls report facing significant and oppressive financial burdens when connecting with one another via ICS telephones. Since ICS phones are the sole legal means of phone communications between inmates and the outside world, we understand the FCC's efforts in evaluating these cost issues.

As for jails and prisons in U.S., the primary mandate and mission of these agencies is, above all, to *safeguard the public.* In their dauntless efforts in pursuit of this goal, jails and prisons have faced, and continue to face, numerous unique challenges — some of them conflicting — in addition to associated risks and costs related to ensuring basic public safety. These risks have, over time, grown larger, and many correctional agencies have grappled with these issues, right along side the pressures felt by inmates and others for greater access at lower costs.

We examine these issues, risks and costs — both from a historical perspective as well as a practical one, and review the solutions available today, both technological solutions as well as policy solutions. An analysis that follows examines the ongoing security concerns related to the ICS, as well as concerns for the safety and well-being of victims and other vulnerable populations (in addition to those of the general public). We also analyze arguments about costs related to ICS security, look at tradeoffs that have been proposed, and explore proposed changes to ICS-related rates — including some that might pose hidden, and potentially deleterious, effects.

Finally, we offer recommendations to the Commission for a balanced approach to the current issue. We respectfully suggest that the needs of victims and other vulnerable populations, and those of the public in general, must be taken into consideration in this matter, just as the needs of inmates and their families have thus far been considered. We discuss the promise of ACTFIRST-level systems to address both security issues as well as scale to meet growing demand.

We conclude with a recommendation that the Commission consider ensuring that the cost of ICS-based security systems be included as part of the rate structures for ICS calls moving forward.

Table of contents

Executive summary 2

1. Introduction 4

2. Victims and Vulnerable Populations 5

2.1 Inmates as a Vulnerable Population 5

3. The Rate Challenges that You Likely Know About… 6

4. …and the Security Challenges that You May Not Know About 6

4.1. Organized Crime & Violence 6
4.2. Fraud, Theft and Other Money-Related Crimes 6
4.3. Drug-Related Crimes 7
4.4. ICS Security Issues 101 7

5. Technology Solutions to ICS Security 8

5.1 ACTFIRST Technology: A Viable Alternative? 9

6. Analysis: How Low is *Too* Low? Security as a Cost Linked to an Inmate Call 10

6.1 The Fundamental Challenges of Caps 10
6.2 The Risk of a Design Solution that Backfires 10

7. Recommendations 11

8. Conclusion 12

9. About the authors 12

10. References 12

1. Introduction

A fact of life for jails, prisons and other correctional institutions in the United States is the statistical reality that, while many inmates abstain from criminal activity while incarcerated, many others do not. Moreover, the inmates bent on conducting criminal activities while incarcerated are well known for doing so in large part *through the ICS* — as the following 1999 case study by the U.S. Department of Justice illustrates (*37*):

Anthony Jones ran a large heroin and cocaine organization in Baltimore, with a penchant for violence. At least ten murders, so it was told, "one in which a man was set on fire" (38). Then, one day in February 1996, Jones was arrested — for being a felon in possession of a firearm. A drug conspiracy indictment followed soon after, in April. Convicted of the former charge in September, Jones received a 37-month federal sentence in November. As Jones began serving his sentence at a federal prison at Allenwood, PA, the Maryland U.S. Attorney was aggressively pursuing a grand jury investigation into Jones' drug conspiracy, planning to supersede the lighter indictment filed in April with a significantly heavier one. The Department of Justice (DOJ) report detailed that

> *This investigation included subpoenas to witnesses and co-conspirators in Jones' drug trafficking organization. Jones became aware of the investigation and also became aware that potential witnesses had been approached by law enforcement to testify against him. Jones used coded language over prison telephones to order his associates to murder two men who he suspected had testified against him. One of the men was killed, the other was shot several times and survived.* (39)

This case study offers a window into a much darker, but surprisingly significant, aspect of inmate telephone access to the outside world. In fact, the DOJ has chronicled hundreds of criminal convictions based on charges involving the use of an Inmate Calling Service (ICS). While more complete accountings of these convictions are detailed in Chapters 2 and 4, inmates have been documented using the ICS to order executions; to continue running crime families or large organized crime operations, to continue their direction of large drug trafficking, manufacturing and distribution enterprises; to order or participate in gang activities, and even to conspire to commit acts of terrorism (41, 42).

Moreover, a disproportionately large percentage of these ICS-enabled crimes target and victimize *vulnerable populations.* Detailed in greater depth in Chapter 2, vulnerable populations tend to consist of victims, witnesses, jurors, inmates and others who have come to the attention of an inmate on their road from free citizen to incarceration. All too often, it is the family members of these individuals who are targeted for threats, extortion and violent crimes.

As will be demonstrated, the fact that the list of vulnerable populations includes inmates adds yet another dimension to this case. Inmates and their families are routinely victimized and harmed in myriad ways by inmates who abuse the ICS for criminal intent. Ultimately, then, effective security of the ICS helps keeps inmates and their loved ones safer, and less prone to the fallout and victimization that such crimes often involve. If, on the other hand, ICS security is shortchanged due to not taking into account the added burden associated with ICS security, inmates and their loved ones may be hurt directly.

A major challenge for correctional facilities, therefore, is the task of monitoring the calls that inmates make.

In order to properly meet this challenge, facilities and ICS providers should, in theory, be required to maintain staffing levels sufficient to monitor every second of every inmate call — to make sure that every attempt by an inmate to use the ICS to commit a crime would be met by an equally dedicated, equally powerful ability to detect such activity (and thus, give law enforcement personnel the intelligence they need to prevent such crimes, and prosecute its perpetrators.) Historically, however, such a massive level of staffing required to monitor all such calls has been prohibitively expensive — despite the known threats to the public in general, and to vulnerable populations in particular, that these calls pose.

Monitoring calls using human listeners turns out to be so impractical (not to mention being tedious, difficult work, requiring unbroken attention for long stretches of time) that no jail or prison has ever been expected to execute it. In fact, a "best practices" mandate from the Federal Bureau of Prisons in 1999 recommended that state and federal prisons aim to monitor a mere *4%* of inmate calls (at random, no less), as a *high bar of achievement* (25).

Thus, quite apart from criminal investigations and other law enforcement activities to prosecute crimes, a key challenge for jails and prisons has been to simply *detect* criminal activities by monitoring the calls that inmates make.

As will be demonstrated herein, the challenge of finding these calls — not prosecuting them, mind you; not even investigating them, but merely *finding them* — has historically proven to be either too technically difficult, too costly — or both — to execute effectively. Only in the past five years has it become not only possible, but actually cost-effective to monitor *all inmate calls,* in order to uncover the most suspicious calls. These calls represent six plus percent of the total and are the calls most likely to involve criminal activities, continued victimization of members of vulnerable populations, and threats to public safety.

A primary goal of this white paper, therefore, is to **raise awareness** about the nature of ICS-related security issues, and attempts at solving those issues with specific inmate telephone security solutions. The security issues have direct impacts on public safety, the safety of these vulnerable populations, as well as the safety of *their* loved ones. And, while many security solutions have been developed and deployed over the years, inmates have found ways to defeat many of these systems. We will highlight these systems, as well as a promising new class of technology-based security systems. These new systems have demonstrated effectiveness at rectifying key security issues.

A secondary goal of this white paper is to **present an argument** about security systems for the ICS — an argument that may not yet have been considered. While the FCC is considering price controls for the costs of calls between inmates and their loved ones, there are remarkably good reasons why any such pricing should include provision for the

cost of key ICS security systems — both now and for the future.

Richard Roy, the former Deputy Commissioner and Inspector General of the New York State Department of Correctional Services from 2001 to 2010, takes a broad view of the current case. "It's understood that families have a burden of high rates in certain localities. On the other hand, there's still a responsibility of corrections departments to maintain public safety and protect victims rights." (22)

Armed with this new information and a deeper understanding of the issues in play with respect to the ICS and its interplay with criminal activities and security, we hope that the FCC will formulate a plan that meets the needs of all concerned.

In order to fully appreciate who is at risk when security falls short, a more complete discussion about targets for criminal behavior using the ICS is in order.

2. Victims and Vulnerable Populations

In the Notice of Proposed Rulemaking (NPRM) portion of the *Inmate Calling Order on Remand and NPRM* (30), the Federal Communications Commission asked "whether the current regulatory regime applicable to the provision of inmate calling services is responsive to the needs of correctional facilities, ICS providers, and inmates, and, if not, whether and how we might address those unmet needs." (43).

In responding to this question, we are compelled to first raise an eyebrow at the wording of the question itself. It is noteworthy to us that any question about the needs of these three groups takes into account only some of the constituencies involved. We appreciate that all three mentioned groups — correctional facilities, ICS providers and inmates — rightfully have needs that can and should be considered in this discussion.

However, we respectfully submit that the question asked in the *Inmate Calling Order on Remand and NPRM* (43) is incomplete without also considering other groups whose needs are also worthy of consideration in this matter. Since concepts such as rate caps for inmate calls raise concerns about the ability of the jails and prisons to secure the ICS on an ongoing basis, the needs of additional groups come into sharp focus.

More specifically, these additional groups include other vulnerable populations such as **victims**, witnesses, jurors, public servants and others in the law enforcement and criminal justice systems — in addition to the inmates and correctional facilities named in the Commission's question.

Individuals join these vulnerable populations when inmates either encounter them personally, or when they are brought to an inmate's attention in the process of the commission of a crime, or on the road to convictions and sentencing, or while incarcerated. For the purposes of this white paper, vulnerable populations may include:

- Crime victims
- Witnesses
- Informants
- Jurors
- Law enforcement personnel
- District attorneys
- Judges
- Correctional officers
- Correctional administrators and staff
- Fellow inmates

Notably, family members of all these individuals may also become targets — which, by definition, makes *them* yet another vulnerable population as well.

The general public has a right to safety and security from harm. But don't the victims of crimes in particular merit some sort of special consideration for relief from further damage or intimidation from their assailants? And what about the witnesses and informants, who may be taking a risk when they agree to testify to protect the public? What about the jurors who determine guilt or innocence, and have historically been subject to threats and extortion before trials, and possible retribution after?

The fact that a disproportionately large percentage of crimes committed using the ICS target victims (41, 42) and other vulnerable populations means that these populations are *all* at risk to be victimized when ICS security systems fail to catch the offenders. What's more, these members of vulnerable populations are not alone in being targeted. Vulnerable populations may include the individuals themselves, or members of their families, or both. Targeting of vulnerable populations has been known to include harassment and re-victimization of victims and their families, intimidation and threatening of informants, witness tampering, intimidation and threatening of witnesses, killing and attempted killing of witnesses (to either prevent testimony or in retaliation); threatening of prosecutors and FBI agents, and retaliation against judges (41, 42). As described by the DOJ in the case of Anthony Jones, individuals may become targets *even if suspected* of deeds they may or may not have done (39).

2.1 Inmates as a Unique Vulnerable Population

The fact that the list of vulnerable populations includes inmates adds yet another dimension to this case.

When correctional officers in prisons and jails are asked about the most frequent, acrimonious complaints they hear from inmates concerning the ICS, their response seldom changes. "If you want to see an inmate get really mad, be around here when one of them finds out their PIN's been stolen," says a Senior Correctional Investigator at a 1,500-inmate state prison in the Northeast (4). "*PIN,"* in this case, stands for the confidential *personal identification number* that an inmate is given when s/he is first enrolled in the inmate calling system. "PIN stealing" occurs when another inmate is able to learn this confidential PIN number, and is thus able to make calls using the stolen ICS account. Since calls tend to be prepaid by inmates' family members, PIN-stealing victims may wake up one morning to find that their phone accounts have been drained.

When inmates use ICS phones to commit crimes, other inmates fall prey. ICS phones have been used in both successful and unsuccessful attempts to intimidate, extort, scam, injure and kill inmates, as well as supply them with drugs. Often the offenders rope other inmates into

involvement, leading to charges of aiding and abetting or conspiracy for these unwitting assistants — charges that can turn a short sentence into a much longer one (26, 41, 42). Ultimately therefore, any shortcomings of security of the ICS phone system hurt inmates and their families directly.

Inmates and others who, in their frustration, argue for rate caps, or parity of ICS rates with civilian phone rates, or other means of removing costs not involved with the service of the call itself, unwittingly do themselves harm. By advocating for these goals, as we will see later on, they are *de facto* advocating for weakening or removing security on the ICS — or at the very least, making further security innovations impractical or unlikely to implement, when jails and prisons find their ICS budgets on a "fixed income."

3. The Rate Challenges that You Likely Know About…

Not just anyone can make a legal phone call that connects an incarcerated inmate with someone from the outside world. Even family members and friends of an inmate are unable to place calls to a correctional facility, such as a jail or a prison, in order to talk to the inmate. Instead, virtually all calls where inmates talk on the phone are outgoing: inmates are the only ones able to place calls. They make their calls within timeframes set by the facilities that house them, often with maximum numbers of calls they can make each week or month. Inmates make these calls at rates set by an ICS provider — a telecommunications company capable of providing such service — with whom the vast majority of correctional institutions in the US will enter into an exclusive contract.

Although inmates must place all calls to communicate with loved ones, they almost never pay for the calls themselves (16). Rather, the cost of those calls are typically borne by inmates' family members — people who, almost by definition, are free and innocent civilians. Statistically, these family members are rarely high wage earners; in reality, members of inmate families often struggle to make ends meet (8).

The family members of those incarcerated, therefore, have limited options. They must wait for the calls to come to them. And when the inmates place their calls, the family members must pay for them.

It's an extremely well-documented phenomenon that the more contact incarcerated inmates have with members of their families and communities, the lower their incidence of recidivism (e.g. 1, 2, 7, 10, 11, 12, 15, 19, 31). While these effects are not as significant as other evidence-based anti-recidivism programs such as education and job training (23, 28), treatment for drug addiction (9, 20), more focused approaches to community re-entry (20) and incentives once paroled (9), inmate contact with loved ones and community members while incarcerated is an important tool in the arsenal to reduce the chance that inmates will return to incarceration in the future.

So when a great outpouring of inmates' family members and friends from across the U.S. complain that the costs of inmate phone calls have become unaffordable for them, it is incumbent on the society as a whole to consider these complaints, take them seriously and, where possible, address them. Not just because the payers are suffering financial hardship, but because the issue is widely known to be *a matter of public safety.* (e.g. 11, 12, 23)

4. …and the Security Challenges that You May *Not* Know About

Ironically, public safety turns out to be a key challenge on the other side of this case as well.

As was highlighted in the Introduction, hundreds of criminal convictions have been documented, transactions for which were completed using ICS telephones (36, 41, 42). In addition to countless charges ranging from contempt, conspiracy, obstruction of justice as well as aiding and abetting, the more notable criminal activities conducted time and again by inmates using the ICS are broken down into four rough categories:

1. Organized Crime and Violence
2. Fraud, Theft and Other Money-Related Crimes
3. Drug-Related Crimes
4. Crimes against Vulnerable Populations

This last category, detailing crimes against vulnerable populations, has already been detailed in Chapter 2. What follows, is a selection of notable criminal convictions in the first three categories:

4.1. Organized Crime & Violence

Racketeering, racketeer influence and corrupt organizations (RICO), violent crimes in aid of racketeering, continuing criminal enterprises, direction of gang activities, explosives, firearms, distribution of weapons, direction of drug enterprises, smuggling, conspiracy to bank robbery, assault, murder, attempted murder, attempt to kill, murder for hire, and conspiracy to commit murder. (36, 41, 42)

4.2. Fraud, Theft and Other Money-Related Crimes

Fraud, bank fraud, mail fraud, wire fraud, credit card fraud, check fraud, tax fraud, Medicare fraud (of $30 million), bookmaking, forgery, money laundering, extortion, loan sharking, counterfeiting, and sale of stolen goods (41, 42).

4.3. Drug-Related Crimes

Drug distribution, drug manufacturing, drug trafficking, drug introduction, drug conspiracy, in addition to myriad other drug offenses. (26, 41, 42).

4.4. ICS Security Issues 101

The above accounting of documented criminal activities notwithstanding, for jails and prisons across the United States, protecting and maintaining public safety is "job #1." Written into the mission statements of state departments of correction

and countless county jails are mandates to "improve public safety" (3, 18); "Protect Society" (29); "Protect the public" (13) and "Provide public safety" (24).

Case in point: Historically, the only way to know if a given inmate was, or was not, speaking on a call, was for a member of the correctional staff to be physically present, in the room, listening to the entirety of it (34). Such comprehensive monitoring was feasible when inmate phones were first introduced at the U.S. Bureau of Prisons in 1973 — when inmates were allowed "at least one telephone call every three months" (40).

Today, however, the notion of manual, one-on-one monitoring of inmate phone calls by correctional officers is simply impractical. For one thing, it is no longer feasible for correctional officers to be physically present to monitor calls. Instead, such monitoring has long been forced to give way to listening via audio only — often after the fact — without the benefit of visual corroboration of identities.

For example, in a medium-sized, 1,000 bed facility, inmates may place 260,000 calls in a given year (14). At a national average inmate call time of 11 minutes, these calls total close to 50,000 hours' worth of calls — equivalent to 25 man-years of labor (14). Labor that, by definition, is extremely tedious and challenging to one's attention. It is also a task for which we humans are *not* ideally suited. Distinguishing between the many possible inmate voices present in a region of a prison, for example, is not something humans typically score well on — even when familiar with all twenty voices (21).

For these and other reasons such as the tremendous growth in incarcerated populations (32), security systems that thoroughly monitor inmate phone calls have historically proven so prohibitively expensive to jails and prisons in the U.S., such monitoring has not been practiced for at least the past 37 years.

Instead, in the intervening decades, correctional facilities in the U.S. have increasingly relied on the *recording* of all inmate calls, the vast majority of which are never listened to. What's more, American jails and prisons have increasingly relied on the inmates themselves to "ID" their own calls. The rationale goes like this: Upon booking in a jail or entering a prison, an inmate is set up with a personal phone account (typically paid for by family members of the inmate) and given a confidential number — a Personal Identification Number, or PIN. The inmate is then directed to use only this account for calling family or friends. The PIN becomes at once a safety feature, to prevent other inmates from abusing their account, and a method of verifying that inmate's identity (e.g., 27).

The trouble is, nothing has prevented inmates from hiding their identities by *sharing* their ICS accounts with other inmates. Often, this "PIN sharing" is voluntary; it may be as simple as one inmate entering their PIN for another inmate, then walking away — in exchange for cigarettes, or a favor, or a similar call with "reversed charges." Sometimes, it's extortion, assault or some other means of shake-down that proves effective in compelling an inmate to use his account (and enter his PIN) for another inmate's call. Still other instances involve "PIN stealing:" an inmate discovers another inmate's PIN on his own, and simply "masquerades" as the other inmate as he pleases. Even when next month's phone bill reveals a drained account to a surprised (and enraged) inmate, there was no simple method to track down the inmate who made those calls.

As mentioned earlier, the funds placed in the inmate's account are almost never supplied by the inmate himself. Instead, the money is typically added to the account by the inmate's family members. Thus, the problem of PIN theft affects inmate family members directly, placing an additional burden on the families. Part of the issue of affordability of inmate calling, then, may be attributed to PIN theft, since family members of such inmate victims are constantly in need of replenishing an account that drains unexpectedly (and unfairly) fast. At facilities where PIN theft is an issue, the ability to discover the perpetrator is often limited, and can take some time to track down if at all.

It's also not uncommon for family members of inmates to be threatened or extorted into silence on such matters. Having stolen another inmate's PIN, the offending inmate may place calls to the victim's family members, promising violence to them or the victim inmate if they are found out, or if the family members don't connect the PIN thief to three-way calls to people the PIN thief wishes to talk to.

Indeed, whether via PIN sharing or PIN stealing, once an inmate has hidden his or her identity, that inmate's activities on the ICS phone are extremely unlikely to be detected. Were this inmate to orchestrate a crime beyond the walls using one of these methods with the ICS, the hidden identity effectively buries any evidence before the crime is detected. Moreover, even if the crime, subsequently committed in the outside world, were to be detected *post facto,* the inmate's now-hidden identity would effectively render the link between the crime and the responsible inmate *untraceable* — unless it were stumbled upon by accident.

For many years, inmates across the country have successfully exploited these methods. They have effectively hidden their identities on calls using traditional ICS phone systems, and proceeded to commit crimes.

But how often do such activities take place? As former Secretary of Defense Donald Rumsfeld famously said, "We don't know what we don't know." For many years, evidence for such crimes was sparse and anecdotal, since without a tip-off, investigators would literally need to stumble across such activities by chance in order to find them. Thus, it has long been a matter of speculation and debate as to how widespread this phenomenon is, given the small number of isolated cases that investigators were historically able to periodically uncover.

With the extent of such problems unknown, and costs to comprehensively monitor them impractical, even highly-regarded correctional agencies have been forced to make choices in the past that only later proved disastrous. As later investigations revealed, these choices came at a great cost, not least in lives of many victims and others in at-risk populations, in addition to the public safety in general. Victims and the public are safer now, as a result of reforms put in place to meet these challenges. Still, many significant security threats related to the ICS remain under-funded and unaddressed at thousands of facilities throughout the country, at all levels.

Until recently, neither correctional facilities nor anyone else had any idea of the actual extent of these problems. However, in the past five years, software systems made by JLG Technologies have since demonstrated that such identity-hiding calls involve close to *seven percent of all inmate calls.* Moreover, the same software systems enable jails and prisons to uncover the true identities of these inmates.

Today, inmates have developed numerous ways to defeat current conventional security systems. Most of these ways involve inmates hiding their identities on calls. Inmates typically hide their identities by sharing PINs with other inmates. As a result, many crimes have been committed, and continue to be committed, using the ICS.

The current situation has been slow and incremental to develop, and the inmates have found very effective ways to avoid detection, so many facilities are not even aware of the issue. Even when a facility stumbles on an ICS-related crime, it is often come across by accident. Thus, it appears to be an isolated incident, instead of part of a large security breach

Even today, comparatively few facilities understand the extent of the problem. Awareness of the issue is slow to migrate to the people who need to hear about it. Those who do understand, and who grasp the implications, tend to advocate for a higher standard of ICS security protection.

Michael Lieberg, Chief of the Criminal Division in the County Attorney's office in Stearns County, Minnesota, appreciates this higher standard. For the past year and a half, Lieberg's team has been working with an ICS-based security system that is part of an entirely new breed of inmate phone monitoring systems. Unlike other ICS-based security systems, this one doesn't overtly validate a call or simply record and play back the call for investigators later on. This system uses artificial intelligence to, in a very real sense, actually to *listen* the call.

Rather than looking for individual words or phrases, this system continuously monitors the inmate voice it hears on the call, comparing that voice to many voice samples of inmates. The entire call, from start to finish, is monitored in seconds — immediately after they are made, screening and analyzing every second of a call. Lieberg notes that when there's a victim involved, inmates tend to actually intensify their criminal activities — and focus them on victims. "Here in Stearns County, our focus has almost always been on domestic and domestic violence-related offenses, where there's an incentive to use a different PIN number. I would say the percentage [of inmates sharing PINs to hide their identity] is vastly higher in that category of cases than, say, someone who's in custody on a check forgery."

We detail this standard in the next section.

5. Technology Solutions to ICS Security

As mentioned previously, the cost of manually monitoring every minute of every inmate call has not been practical for decades. The sheer volume of inmate phone calls at jails and prisons today dwarfs the ability of the manpower at these facilities to listen to such calls. As a result, only a small fraction of calls made by inmates using the ICS are generally listened to by correctional staff in most modern jails and prisons. Moreover, most of these calls tend to be listened to at random. Finally, what call monitoring does occur is done via audio only — to recorded conversations after the fact — putting the facility at a tremendous disadvantage for positively identifying the inmate (or inmates) actually speaking on the call (21).

As has been shown, inmates have long leveraged these disadvantages to defeat the security systems put in place on the ICS. With budgets that are typically tight, correctional staff are often overwhelmed with the amount of work they face, in an uphill battle to take back control of inmate phone security systems.

With the explosion of digital audio technology in commercial, consumer and government sectors in recent years, new hope to address these problems and burdens has appeared. Increasingly sophisticated technology has been developed and implemented for security of the ICS at some jails and prisons in the U.S. — technology that shows real promise.

For a technological solution to the aforementioned challenges to be effective, however, it must overcome several hurdles:

1. The technology must be **automated**. It must be able to monitor all calls comprehensively, regardless of how many inmates are at the facility, how many calls they make, or how long they are allowed to talk.
2. It must offer effective ways to **identify** those inmates who are using the ICS to harm the public. It's simply too easy for inmates to bury their identities on the ICS at most facilities.
3. It should **notify** correctional staff of the calls where inmates are trying to hide their identities, as well as identify and report other patterns of suspicious inmate calls, such as those that include three-way calls.
4. Such technology must be **fast**. Prisons and jails can't wait for weeks, days, or even hours after a suspicious call has been made before receiving a report on it. To be effective at stopping crime, law enforcement needs to know about it immediately. Thus, a technological solution must yield results within seconds — a few minutes at the most.
5. The technology must be **effective** at finding cases of PIN theft as well as PIN stealing.
6. The technology must be **affordable**. Given the current challenges of affordability for inmate calls, an effective technological solution should contribute to *lowering* the overall cost for making ICSs more secure.

In recent years, new biometrics-based technologies have been developed, tested and implemented that have been shown to be effective at monitoring and controlling key aspects of inmate calls — and doing so automatically.

It should be pointed out that all biometric technologies are *not* created equal. As will be seen, some biometrics technologies are relatively unsophisticated, provide limited security and are not difficult for inmates to defeat, as will be shown, more recent technologies that also use biometrics have been demonstrated to be more effective, and more difficult to defeat, than others.

This newer technology has enabled agencies to monitor inmate phone calls much less expensively — and monitor them with much greater coverage than the 4% minimum

threshold for inmate call monitoring mandated by the Department of Justice fourteen years ago (25). Indeed, a new breed of automated inmate phone call monitoring systems is now capable of analyzing *every second of every inmate call,* reporting and notifying correctional personnel of questionable calls within seconds. And, while some aspects of automated call monitoring fall short of human capabilities (such as in areas like word or phrase recognition and meaning understanding), many other aspects of this technology actually *exceed* human capabilities.

For example, this biometric system is designed to analyze and determine the true identity of the inmate or inmates on a call, based solely on their voices. The system actually *exceeds* the speed and accuracy of humans to accomplish the same task *by at least 70 times* (14). Further, the same system is capable of finding the calls on which inmates have been trying to hide their identities, and bring those calls to the attention of corrections investigators.

Because this threat has been so great, many companies have wrestled with this problem for the past 20 years. Automated solutions to the challenge of monitoring inmate phone calls include a wide variety of *biometrics technologies* (technologies that record, compare and measure biologically-based artifacts that distinguish one person from another, such as fingerprints, retinal patterns, or how one speaks), many of which have been tried in facilities throughout the United States.

In brief, biometrics technologies relevant to the ICS tend to fall into two broad categories: The first category employs conventional means of capturing, and sometimes verifying, aspects of an inmate's ID. Examples of such biometric technologies include cameras, fingerprint recognition, bracelets that have unique, built-in radio-frequency identification (RFID) tags, and retinal scanners**.** Notably, all these technologies but the cameras have been proven to be ineffective at inmate facilities. Retinal scanners and fingerprint ID devices are simply too expensive for correctional budgets, and RFID bracelets are simply too easy for inmates to defeat.

The second category of biometric technologies monitor and analyze audio. Such systems can "listen" to the human voice to verify, or even *identify,* the speakers on the call.

Voice-based biometrics, as this latter category is known, has traditionally meant one thing to jails and prisons in recent decades: *Pre-call Biometric Voice Validation,* or simply *pre-call validation*. At the beginning of an ICS call, an inmate at a facility with pre-call validation speaks his or her name, and one or more other phrases. The system compares these phrases with pre-recorded versions that the inmate initially recorded. If there's a match, the call goes through. If there isn't, the call is disconnected.

While pre-call validation has been shown to put a stop to inmates intent on *stealing* the PIN numbers of other inmates (since the inmate who owns the PIN number must be present at the start of the call) the rest of the call is not monitored at all. Thus, nothing now prevents the now-validated inmate from handing the receiver to another inmate, leaving the call primed for PIN *sharing*. This second inmate is then free to talk about any subject, to anyone who might have "stopped by" to be on the receiving end of the call. Or, if the call recipient is amenable, the second inmate can now talk to anyone *else* that the call recipient might have set up a conference call with, or a 3-way call, or simply put the call on speaker, and have another speaker phone nearby with someone on *that* line that this second inmate wishes to speak with. Using pre-call validation, anything can happen after the validated PIN owner hands the receiver over, since the second inmate's identity is never associated with the call. And, with the enormous volume of calls generated at any given facility, this call will, more than likely, quickly slip into oblivion. Safe, safe oblivion.

Another type of voice biometrics is called "Periodic Voice Validation." This strategy includes pre-call validation, but then asks for "re-validation" periodically throughout the rest of the call. Such technology is similarly easy to defeat, for instead of the validating inmate walking away after the pre-call validation, s/he remains close by, ready to hop back on the call whenever the system cuts in to request re-validation.

5.1 ACTFIRST Technology: A Viable Alternative?

Automated, Comprehensive Telephone Identity Resolution Security Technology, or ACTFIRST, is a new way of approaching the threat of ICS-related criminal activities as well as threats to at-risk populations and the general public.

ACTFIRST-level technology must be capable of continuously "listening" to every second of every inmate call, and detecting the identity of every inmate who speaks on a call. The value of such technology is that it can detect mismatches between inmates who *should* be on a call, and those who shouldn't. It is also capable of detecting & reporting patterns of phone system abuse, attempted abuse or likely abuse — all of which often suggest criminal activity. ACTFIRST technology identifies suspected abusers, and provides correctional agencies with an automated list of calls that are most likely to contain threats to vulnerable populations and public safety.

One example of ACTFIRST-level security is the *Investigator Pro,* a software system designed and produced by JLG Technologies of Framingham Massachusetts. Described as an "inmate phone crime detection and prevention system" The *Investigator Pro* was first released in 2007. It was adapted from the results of breakthrough research in automated voice identification — detecting who is speaking on a call — over the course of the entire phone call. The research was conducted by the U.S. Department of Defense, along with some of the worlds foremost experts in the field, over the course of the past 16 years.

The *Investigator Pro* system employs this technology to comprehensively monitor all inmate calls, from start to finish. The system is capable of identifying inmates who try to hide their identities to engage in criminal activity. The system uses the results of this analysis to automatically flag criminal calling patterns, as well as other patterns of suspicious calls, such as 3-way calls. In doing so, the *Investigator Pro* enables investigators to respond proactively to preempt and unravel criminal activity — in many cases, before the criminal activity can manifest itself as harm to vulnerable populations or the public.

Currently, JLG's ACTFIRST systems are continuously monitoring all calls made by more than 80,000 inmates, in the 150 jails and prisons where the system is installed across the United States. To date, the *Investigator Pro* has monitored all

calls made by close to a million inmates — nearly 50 million calls — that total over *9 million hours* of phone calls.

Out of all those calls, the Investigator Pro system has uncovered over 3.25 million suspicious calls — calls in which inmate voices heard on a call did not match the calling inmate's voice, as well as "three-way" calls — and alerted staff at the prisons and jails where they occurred to every one of them.

One correctional officer at a 1,400 bed inmate facility in the Southeastern US has been using the ACTFIRST *Investigator Pro* for close to 2 years. His name and other details are withheld due to ongoing investigations. He heads investigations for the facility, and he had this to say: "I can't even explain how lucky we are to have this system. It's brought the calls we want to listen to to our attention, but It's helped victims stop being harassed. It's helped stop drugs from coming into the jail. With *Pro,* a lot of our high-profile cases have turned into convictions. And even some of our low-profile cases have turned into high-profile cases." (5)

The system has proven to be not only effective — correctional facilities that try it almost universally insist on it in subsequent years — it also has proven highly cost-effective. Its total cost is about 2¢ per minute, or about 25¢ per-call.

6. Analysis: How Low is *Too* Low?

Security as a Cost Linked to an Inmate Call

As we have seen, critical elements of ICS-based security have proven to be a huge challenge for a long time. Agencies have tried myriad solutions to address these issues over the years, but with limited success. Agencies that use Pre-Call Biometric Voice Verification, for example, have been able to control the problem of PIN stealing. But even at such agencies, PIN sharing-related crimes remain rampant.

ACTFIRST technology represents a new technological breakthrough in monitoring calls. Rather than "listening" for a few fixed phrases at the start of a call (as Pre-Call Biometric Voice Verification does, for example), ACTFIRST listens to every second of every call. It's fast, accurate, intelligent and inexpensive, and it reports suspicious calls, including PIN sharing and PIN stealing. In so doing, it shows promise to solve the security holes that have existed for so long.

6.1 The Risk of a Design Solution that Backfires

For Richard Roy, the retired New York State Deputy Commissioner, the calculus for correctional agencies is straightforward.

First, the mission of jails and prisons is to "protect those vulnerable populations — victims, witnesses, and the general public." (22)

Second, if jails or prisons are put in the position of not having sufficient funds to secure the ICS, they may not have any other choice other than to limit inmate access to their ICS.

Historically, this scenario has already played out. In 1983, upon discovering the extent of security breaches posed by their ICS, the FBOP determined they did not have the resources to address the issues. Their response was to significantly cut back the amount of calls that inmates could make (35).

Says Mike Lieberg, "If it was going to cost us more to have a monitoring system than we could recoup in costs from the inmates," says Lieberg, "absolutely we may be advocating to our sheriff's department to limit the times the phones are available [to inmates], as a security measure." (17)

The goal of fostering more contact between inmates and their loved ones is a laudable one. If the FCC chooses to decouple the cost of the ICS from the cost of *security* for the ICS we believe it is highly probable that the net result will be that correctional agencies will be forced to significantly reduce inmate access to phones based on their government ordered mission of protecting the public safety.

It's clear that, in this era of sequesters and tightened budgets, correctional facilities will have few resources to be able to make up the difference between these costs. In the absence of funding to secure the ICS, jails and prisons will do what they need to do to maintain *at least* the level of security they believe is as high as it is at present, or pursue a level that is higher. Sacrificing security, for law enforcement agencies mandated to protect the public, is simply not an option. On the other hand, for these agencies, sacrificing inmates' access to ICS phones is a solution they may be forced to put into place.

As Stearns County Attorney's Office Chief Lieberg puts it, "If we're going to incarcerate somebody, we're obligated as taxpayers to provide for their basic needs. I understand that. We have to pay for their medical, we have to pay for their food, even their clothing — we have to pay for all those things that provide for their basic needs.

"But," adds Lieberg, "as far as I'm aware, there is no case law that says that access to a phone is somehow a fundamental right of every citizen, regardless of incarceration, such that we have to pass that cost on to taxpayers." (17)

7. Recommendations

As we have shown, the benefits of monitoring all inmate calls are many.

We ask the FCC to take the costs associated with implementing and maintaining effective ICS security systems — especially those that can identify the inmate calls which are statistically most likely to be harmful to the public — into consideration when setting new inmate phone calling rates.

We ask that its policy for setting ICS phone rates include specific rate options for technologies that include monitoring capabilities. JLG Technologies' *Investigator Pro* product is just one example of ACTFIRST technologies that can be deployed in identifying suspicious phone calls made by inmates. While other solutions may vary in cost and effectiveness, we believe it is imperative that at least one effective, comprehensive ACTFIRST-level security solution be linked to the ICS — regardless of who makes it.

As mentioned earlier, we believe that it is a matter of great importance for the FCC to take both victim safety as well as public safety into account as these issues affect ICS rates

(albeit minimally, as discussed above). We also believe that it is in the best interests of victims, other at-risk populations, and the general public at large, that a portion of the actual cost for inmate phone services is devoted to ensuring that inmates are not harming the public when placing their phone calls.

It has been proven by the analysis of more than 50 million phone calls at state and county correctional facilities that more than 6% of all inmate calls are suspicious. Today, there is relatively low cost proven technology to automatically identify these calls, as such, we believe that the cost of an inmate call should include the cost of technology to help keep the public safe.

If the FCC opts to exclude fees that provide for security systems that automatically identify statistically likely harmful inmate calls to the public, we believe that the FCC will be putting the public at risk.

Telecommunications technology is a swiftly-developing sector. ICS phone monitoring technologies that might aid the safety of the public and inmates alike are ever evolving, with new ones being created and developed all the time. In light of this dynamic nature of such technologies, and the new ways that inmates develop to threaten the public safety, we ask the FCC to consider the creation of a review process within the Commission, such that technological improvements may be evaluated and either approved or denied. When new technologies for improving the safety of victims and other target populations are periodically developed, or existing ones are refined, such a review process would enable the FCC to be able to take such developments into consideration.

ACTFIRST technology benefits inmates, makes them safer, makes their phone accounts less prone to theft, makes them less vulnerable to threats and extortion.

When considering the rate structure for inmate calls, funds need to be carved out for security. Further, that “carve-out” needs to be kept flexible from year to year, in order to account for changes in facility population, demographics that might change from year to year, and new technological improvements to security as they become available.

Richard Roy sums up our recommendations succinctly: “There needs to be a balanced approach. In this case, we need to raise awareness that there is a need for telephone security, as well as the ability of correctional agencies to provide that security on an ongoing basis for employees, victims, witnesses, inmates, and the general public.” (22)

We understand the FCC’s mission to establish a “fair” rate in this area. We believe that, as a result of the FCC investigation, the FCC will find effective ways to address issues related to inmate phone call rates. We respectfully ask the FCC to also take into account the public safety aspects of ICSs during its rate setting policy formulation.

Finally, ACTFIRST systems provide protection to inmates and their families by protecting them from the theft of funds and debit card money.

Because they are automated and designed to screen inmate calls at correctional facilities, ACTFIRST systems also reduce labor costs at jails and prisons. At facilities that monitor even a fraction of inmate phone calls today, an ACTFIRST system can greatly reduce the amount of calls that the facility needs to listen to. When listening to calls, systems like the *Investigator Pro* provide a wide range of tools for correctional officers to further reduce the amount of time required. The ability to skip pauses, for instance, or speed up the call (without sacrificing clarity) are two ways that the system saves time and manpower required to monitor these phone calls.

Stearns County, MN, for example, has been using the Investigator Pro for the past year and a half. They recently reported that they had 634 hours of phone calls they knew they needed to listen to. Using the *Investigator Pro,* it took their staff 64 hours to complete this task — for a total of a 90% savings in time and manpower. JLG Technologies notes that, on average, the amount of time saved when listening to calls is typically in the range of 50% to 70%. In other words, 100 hours of inmate calls takes between 30 and 50 hours for correctional staff to listen to, with complete effectiveness (14).

Said Tim Couloumbe, Investigator at the New Hampshire Department of Corrections, “The *Investigator Pro* has greatly reduced the amount of time I have to spend listening to calls.” (6)

8. Conclusion

We respect and acknowledge the challenges before the FCC as it evaluates a new rate structure for inmate calls.

We believe this white paper shines an important light on the public safety issues associated with inmate phones. We trust that now that the FCC has been provided with detailed information into some of the key public safety aspects of inmate phone calling, that the FCC will also take into account the safety of the crime victims, the witnesses, the jurors, the public servants and other vulnerable populations, as well as all of *their* loved ones — in addition to the safety of the general public.

We are confident that, armed with the full spectrum of information that includes not only rates and costs but also key security issues and known threats to public safety, the FCC will consider solutions that bear all such costs in mind.

9. About the Authors

Jonathan Klein is a multi-disciplinary technology designer and journalist in the Boston area. Founder of the independent consulting firm Graffectivity LLC, he has helped design advanced user interfaces for correctional security systems for 6 years, including ACTFIRST-level systems as an independent consultant to JLG Technologies. In addition, he has designed advanced user interfaces for the U.S. Army’s PackBot tactical robot, as well as Vecna Technologies' prototype Battlefield Extraction-Assist Robot (BEAR).

JLG Technologies is an independent, privately-held company based in Framingham, MA. It is not owned in whole or in part by any ICS provider. It provides security products and services to ICS providers on an independent basis.

10. References

1. Adams, D., & Fischer, J. (1976). The effects of prison residents' community contacts on recidivism rates. *Corrective and Social Psychiatry , 22* (4), 21-27.

2. Bales, W. D., & Mears, D. P. (2008). Inmate Social Ties and the Transition to Society: Does Visitation Reduce Recidivism? *Journal of Research in Crime and Delinquency , 45* (3), 287-321.

3. California Department of Corrections and Rehabilitation. (2013). *Mission Statement, Vision, Mission, Values, and Goals*. Available at the California Department of Corrections and Rehabilitation website at: http://www.cdcr.ca.gov/About_CDCR/vision-mission-values.html

4. Correctional Investigator in Northeast (name withheld), (2008). *Personal Interview.* Interview conducted by the author with a Senior Correctional Investigator at 1,500-bed state prison facility in the Northeastern United States (details withheld due to request of facility), on site, April 8, 2008.

5. Correctional Investigator in Southeast (name withheld). (2013). *Personal Interview.* Conducted by the author with Correctional Investigator at 1,400-bed state jail in the Southeastern United States (details withheld due to sensitivity of pending investigations), by telephone, July 9, 2013.

6. Couloumbe, Timothy, Cpl. (2011). *Personal Interview.* Conducted by the author with a Correctional Investigator at the 2,600-bed prison system in the State of New Hampshire Department of Corrections, Concord, NH, by telephone, October 26, 2011.

7. Duwe, G., & Clark, V. (2013). Blessed Be the Social Tie That Binds: The Effects of Prison Visitation on Offender Recidivism . *Criminal Justice Policy Review , 24*, 271-296.

8. Ellison, K. (2012, October 2). *Letter to FCC Chairman Re: Inmate Phone Rates.* Available at the Democracy In Action website at: https://org2.democracyinaction.org/o/6220/images/Letter%20to%20FCC%20Chairman%20re%20Prison%20Phone%20Rates.pdf

9. Florida Department of Corrections Office of Re-entry. (2009, July). *Increase Public Safety by Reducing Recidivism.* Available from the Florida Department of Corrections website at: http://www.dc.state.fl.us/orginfo/ReducingRecidivismExecutiveBriefingFINALbook062009.pdf

10. Glaser, D. (1969). *The effectiveness of a prison and parole system* (Abridged ed.). Indianapolis, IN: Bobb-Merrill.

11. Hairston, C. F. (2002, April). The importance of families in prisoners' community reentry. *ICCA Journal on Community Corrections* , 11-14.

12. Holt, N., & Miller, D. (1972). *Explorations in inmate-family relationships.* Research Division. Sacramento: California Department of Corrections.

13. Illinois Department of Corrections. (2013). *Mission Statement, Agency Overview: About the Illinois Department of Corrections.* Available at the Illinois Department of Corrections website at: http://www2.illinois.gov/idoc/aboutus/Pages/IDOCOverview.aspx

14. JLG Technologies, LLC (2013). Unpublished statistics from historical inmate phone call monitoring data. July 5, 2013.

15. Klein, S. R., Bartholomew, G. S., & Hibbert, J. (2002). Inmate family functioning. *International Journal of Offender Therapy and Comparative Criminology,* 46 (1), 95-111.

16. La Vigne, N. G., Naser, R. L., Brooks, L. E., & Castro, J. L. (2005). Examining the Effect of Incarceration and In-Prison Family Contact on Prisoners' Family Relationships. *Journal of Contemporary Criminal Justice, 21* (4).

17. Lieberg, M. (2013). *Personal Interview.* Conducted by the author with Michael Lieberg, current Chief of the Criminal Division in the County Attorney's office in Stearns County, Minnesota, by telephone, June 20, 2013.

18. New York State Department of Corrections and Community Supervision. (2013). *Mission Statement, The Departmental Mission*. Available at the New York State Department of Corrections and Community Supervision website at: http://www.doccs.ny.gov/mission.html

19. Ohlin, L. (1954). *The stability and validity of parole experience tables.* University of Chicago.

20. Pew Center on the States. (2011, April). *State of Recidivism: The Revolving Door of America's Prisons's Public Safety.* Available at the Pew Center on the States Performance Project website at: http://www.pewtrusts.org/our_work_report_detail.aspx?id=85899358613

21. Piesing, M. (2013). The race to fingerprint the human voice. *The Independent,* February 13, 2013, at para. 3. Available at: http://www.independent.co.uk/news/science/the-race-to-fingerprint-the-human-voice-8493867.html

22. Roy, R. (2013). *Personal Interview.* Conducted by the author with Richard Roy, Deputy Commissioner and Inspector General of the New York State Department of Correctional Services from 2001 to 2010, by telephone, June 19, 2013.

23. Steurer, S. J., & Smith, L. G. (2003, February). *Education Reduces Crime: A Three-State Recidivism Study.* Available at the Correctional Educational Association website at: http://www.ceanational.org/PDFs/EdReducesCrime.pdf

24. Texas Department of Criminal Justice. (2013). *Mission Statement, Texas Department of Criminal Justice Offender Orientation Handbook.* Available at the Texas Department of Criminal Justice website at: http://www.tdcj.state.tx.us/documents/Offender_Orientation_Handbook_English.pdf

25. United States Department of Justice / Office of the Inspector General. (1999). *U.S. DOJ / OIG Special Report: Criminal Calls: A Review of the Bureau of Prisons' Management of Inmate Telephone Privileges* (August, 1999) at Chapter 2: Federal Inmate Access to Telephones at 2.2: History of Inmate Access to Telephones, at para. 1 (1999 DOJ/OIG Special Report). Available at the U.S. DOJ website at: www.justice.gov/oig/special/9908/callsp2.htm#History

26. United States Department of Justice / Office of the Inspector General. (2003, January). *The Federal Bureau of Prisons' Drug Interdiction Activities.* Available at the U.S. Department of Justice website at: http://www.justice.gov/oig/special/9908/

27. United States Federal Bureau of Prisons. (2013). *Federal Prison Inmate Handbook* at 24. Available at the U.S. Federal Bureau of Prisons official website at: http://www.bop.gov/locations/institutions/ben/BEN_aohandbook.pdf

28. United States Federal Bureau of Prisons. (2013). *Inmate Matters.* Available at the U.S. Federal Bureau of Prisons official website at: http://www.bop.gov/inmate_program

29. United States Federal Bureau of Prisons. (2013). *Mission Statement, Mission and Vision of the Bureau of Prisons*. Available at the U.S. Federal Bureau of Prisons official website at: http://www.bop.gov/about/mission.jsp

30. United States Federal Communications Commission (2002). *Implementation of the Pay Telephone Reclassification and Compensation Provisions of the Telecommunications Act of 1996, CC Docket No. 96-128, Order on Remand & Notice of Proposed Rulemaking,* 17 FCC Rcd 3248 at 3276, para. 72 (Inmate Calling Order on Remand and NPRM).

31. United States Federal Communications Commission (2012). *Notice of Proposed Rulemaking: In the Matter of Rates for Interstate Inmate Calling Services* (WTC 12-375) at 3, #4 (2012 FCC NPRM) available at http://www.fcc.gov/document/rates-interstate-inmate-calling-services

32. United States Government Accountability Office (2012). *Bureau of Prisons: Growing Inmate Crowding Negatively Affects Inmates, Staff, and Infrastructure* at 21 (2012 GAO Report) available at http://www.gao.gov/assets/650/648123.pdf

33. Wright, M. et al (2007). Implementation of the Pay Telephone Reclassification and Compensation Provisions of the Telecommunications Act of 1996, *Petitioners' Alternative Rulemaking Proposal,* CC Docket No. 96-128, at 4-6 (filed Mar. 1, 2007) (Alternative Wright Petition)

34. *1999 DOJ/OIG Special Report* at Chapter 2, Part 2.2: History of Inmate Access to Telephones. Available at:www.justice.gov/oig/special/9908/callsp2.htm#History

35. *1999 DOJ/OIG Special Report* at Chapter 2: Federal Inmate Access to Telephones at 2.3: Inmate Telephone Abuse and the BOP 's Early Responses. Available at: http://www.justice.gov/oig/special/9908/callsp2.htm

36. *1999 DOJ/OIG Special Report* at Chapter 4: OIG Review of Inmate Telephone Abuse. Available at: http://www.justice.gov/oig/special/9908/callsp4.htm

37. *1999 DOJ/OIG Special Report* at Chapter 5: OIG Case Studies of Inmate Telephone Abuse; Part 2: Anthony Jones. Available at the U.S. DOJ website at: http://www.justice.gov/oig/special/9908/callsp51.htm

38. *1999 DOJ/OIG Special Report* at Chapter 5: OIG Case Studies of Inmate Telephone Abuse; Part 2, Anthony Jones at para. 3.

39. *1999 DOJ/OIG Special Report* at Chapter 5: OIG Case Studies of Inmate Telephone Abuse; Part 2, Anthony Jones, para. 4.

40. *1999 DOJ/OIG Special Report* at Ch. 9, Conclusions. Available at the U.S. DOJ website at: http://www.justice.gov/oig/special/9908

41. *1999 DOJ/OIG Special Report* at Table 2: Federal Prosecutions of Cases Involving Inmates Using the Telephone to Facilitate a Crime. Available at the U.S. DOJ website at: http://www.justice.gov/oig/special/9908/table2.htm

42. *1999 DOJ/OIG Special Report* at Table 3: Federal Prosecutions of Cases Involving Inmates Using the Telephone to Facilitate a Crime. Available at: http://www.justice.gov/oig/special/9908/table3.htm

43. *2012 FCC NPRM* at 6, #10.

44. *2012 FCC NPRM* at 10, #22.

JLG Technologies, LLC

Investigator Pro™ Cost Information

July 17, 2013

In response to:

FCC Docket No. 12-375, Rates for Interstate Calling Services

Comments in Response to DA 13-1446

Comments in Response to DA 13-1446

The following cost information is being provided to the FCC for JLG Technologies Investigator Pro product. The Investigator Pro product is licensed to ICS providers through JLG Technologies for the purpose of reducing the threats posed by inmate phone calls. The Investigator Pro is designed to automatically identify high risk (high probability of criminal activities) phone calls. It also provides features that substantially reduce the labor costs associated with listening and identifying high risk phone calls.

The following pages are designed to provide the FCC with cost detail in order to assist the FCC in establishing an appropriate rate for the Investigator Pro service.

JLG Technologies, LLC.

Product:	Investigator Pro - Correctional/Prison Telephone investigative productivity tool using continous speaker identification voice biometric technology licensed/commericialized from MIT/DOD

Item	**2012 JLG Operating Statiscs**
Inmate Minutes processed	[redacted]
Inmate Calls processed	[redacted]
Total Inmates	[redacted]
Locations Deployed	140
Agencies Deployed	86
Inmate Calling System Partners	4
Year Product First Released	2007
Company Location	119 Herbert Street, Framingham, MA

Investigator Pro Cost Summary	
Option 1:	Investigator Pro Cost per minute
ICS Partner performs enrollment	$0.0193
Option 2:	
JLG performs supervised enrollment @ 100 inmates per day ($8.50 per day per inmate), repayed (straighline) over 3.1 years	$0.0210

Costing Process

1. Took 2012 JLG Technologies P&L and map to cost Categories
2. Annualized 2012 cost to account for in year hires.
3. Adjust cost to reflect increases in operating cost (add hires, COGS/Royalties, other operating cost)

JLG Technologies Going-Concern Operating Cost

Partner (ICS) performs enrollment

Cost Categories	Expense	Per Incr ADP	Per Min	Per Call	Per Licensed ADP
Sales	[redacted]	8.2007	0.002416	0.027922218	3.8607807
Marketing	[redacted]	8.4327	0.002484	0.028712134	3.9700018
Business Development	[redacted]	0.3736	0.000110	0.00127215	0.1758991
Support	[redacted]	4.4593	0.001477	0.017067631	2.3599266
Sustaining Engineering	[redacted]	4.3310	0.001434	0.016576582	2.2920296
Research, Development, Engring	[redacted]	19.0694	0.006315	0.072986377	10.0917628
Patent Expense	[redacted]	0.1366	0.000045	0.000522647	0.0722659
G&A	[redacted]	3.2292	0.001069	0.012359509	1.7089385
Professional Fees	[redacted]	1.7093	0.000566	0.006542298	0.9045979
Investigator Training	[redacted]	2.7933	0.000925	0.010690917	1.4782238
Services (Implementation)	[redacted]	3.6973	0.001224	0.014151131	1.9566646
MIT Royalty Expense	[redacted]	2.1855	0.000724	0.008364729	1.1565838
Patent Royalty	[redacted]	1.3521	0.000448	0.005175093	0.7155557
Enrollment (ICS Optional)	-	-	-	-	-
Capital Recovery	[redacted]	0.1922	0.000064	0.000735454	0.1016906
Totals	[redacted]	60.1621	0.019302	0.223079	30.844921

Per Minute Cost	0.019302

Notes:

Includes hiring of;
National Sales Mgr
Technical Support/Service Mgr
Support Technician
Accountant PT
Product Manager
Tech Writer PT
Software QA
Assumes partner does supervised enrollments

JLG Going-Concern Operating Cost

JLG performs supervised enrollment

Cost Categories	Expense	Per Incr ADP	Per Min	Per Call	Per Licensed ADP
Sales	[redacted]	8.2007	0.002416	0.027922218	3.8607807
Marketing	[redacted]	8.4327	0.002484	0.028712134	3.9700018
Business Development	[redacted]	0.3736	0.000110	0.00127215	0.1758991
Support	[redacted]	4.4593	0.001477	0.017067631	2.3599266
Sustaining Engineering	[redacted]	4.3310	0.001434	0.016576582	2.2920296
R&D	[redacted]	19.0694	0.006315	0.072986377	10.0917628
Patent Expense	[redacted]	0.1366	0.000045	0.000522647	0.0722659
G&A	[redacted]	3.2292	0.001069	0.012359509	1.7089385
Professional Fees	[redacted]	1.7093	0.000566	0.006542298	0.9045979
Investigator Training	[redacted]	2.7933	0.000925	0.010690917	1.4782238
Services (Implementation)	[redacted]	3.6973	0.001224	0.014151131	1.9566646
MIT Royalty Expense	[redacted]	2.1855	0.000724	0.008364729	1.1565838
Patent Royalty	[redacted]	1.3521	0.000448	0.005175093	0.7155557
Enrollment (ICS Optional)	[redacted]	2.7568	0.000812	0.009386383	1.2978470
Capital Recovery	[redacted]	0.1922	0.000064	0.000735454	0.1016906
Totals	[redacted]	62.918900	0.020114	0.232465	32.142768

Per minute cost	0.0201

Notes:

Includes hiring of;
National Sales Mgr
Technical Support/Service Mgr
Support Technician
Accountant PT
Product Manager
Tech Writer PT
Software QA

JLG does supervised enrollments

Notes on terminology:

ADP – Average (inmate) Daily Population, an industry standard way of looking at inmate population

Supervised Enrollment – A supervised enrollment is the act of obtaining a 30 second voice sample from an inmate where the enroller is sure that the inmate that is enrolling matches the PIN assigned.

MIT – Massachusetts Institute of Technology

R&D – Research and Development

Other Notes:

Enrollment cost run [redacted] per inmate. Cost recovery for enrollments were spread over 37 months for the purposes of the model. The cost to 50,000 inmates was used for the model.