Hoyos Integrity Corporation
1975 E Sunrise Blvd.
4th Floor
Fort Lauderdale, Fla
33304

MY VISION TO PROTECT OUR SECURITY AND PRIVACY

By: Hector T. Hoyos - Founder, Executive Chairman, CEO, CTO

Vision is important as it drives everything. If the vision is correct, the proper experienced human capital is in place, the leadership and team know how to execute operations, and the venture is properly funded, its mission will succeed.

BUT FIRST: beware of false prophets. The cyber security industry is full of them, especially when it comes to the claims of a secure smartphone. My advisors would prefer that I not point this out because it could be perceived as an "attack" against my competitors. I have no competitors! I make a choice to tell it like it is. The fact is that every single company (you can see a table of these on our site) that has attempted to build and deliver to the market a secure smartphone has failed-ALL OF THEM!!! Their promises to do so in the future are futile and will not succeed. I explain the reasons for this below.

Why am I embarking on this venture? Many who know me and are familiar with my track record know that most of my life has been dedicated to creating technologies that keep our military, enterprises, and people safe. I want to protect the world by protecting its people and organizations, their property, security, and privacy. If our team can accomplish this successfully as per my vision, significant financial rewards will ensue for **everyone** involved, including you. Of equal importance to my team and me, is the personal sense of accomplishment of having done a job well done that changes the world for the better.

The biggest problem in existence today…is the security of our information/data-our digital assets. If our information is tampered with or intercepted by bad actors/hackers with interests contrary to our own, our personal and/or professional position is jeopardized, with possible dire consequences.

Think about how we communicate today: Smartphones! Communication between family members, executives within an enterprise, government employees within their agencies, and even the military on the battlefield, have all become necessarily dependent on this practical yet absolutely insecure means of communication. Smartphones are the common denominator to everyone today including attackers or hackers. Yet mobile phones were never meant to be secure. Back in the day when mobile phones were invented no one ever really considered security, these were just devices to make calls. As technology developed, off-the-shelf chips and unsecure operating systems were quickly built into these devices to allow users to carry a slice of their "digital life" inside their phones. Today, calls are what you do least on your mobile. Your *actual* life takes place inside your mobile, yet the lack of security is the norm exposing you to the whole world having unfettered access not only to your digital assets -your emails, texts, calls, pictures, documents, but your physical assets – your bank accounts, credit, etc. As cryptocurrencies develop, this will just get worse.

Nothing you do or store on your mobile is safe or private. The situation worsened when enterprise organizations and government agencies naively allowed mobile devices into their enterprise systems, infecting them, which

many are regretting and now reversing. Even if you encrypt your data on your mobile (to code it using some form of coding/encryption software), it will never be safe, regardless of what encryption vendors or the security industry tell you. Why? Encryption software works inside the memory of your device, which is the same place that hackers, unbeknownst to you, penetrate to deploy something called “ram scraper malware” (bad software meant to steal anything that gets into memory). Encryption happens in memory, but the second anything goes into memory it will be misappropriated by the ram scraper malware and sent outside your mobile to a hacker, before anything is ever encrypted. Yes, your data will be encrypted, but after it has been stolen; hence, encryption is useless as it is conceived and sold, and the industry knows it.

There are many chip manufacturers and they all have similar security problems. To illustrate the problem, I will focus on the biggest of them, which ships hundreds of millions of chips/year: San Diego-based Qualcomm. It manufactures its own chips from an architecture design from a British-based company called ARM. Think of a chip's architecture just like the architecture of a building. In a building design you have the foundation, plumbing, electric, rooms, etc. Inside a chip you have similar structures, and one of those is a "room" called Trust Zone. Think of a panic room inside your house meant to keep your family safe by securely locking them inside in case of a home invasion. The Trust Zone is designed inside the chip for chipmakers to keep part of the operating system inside and for device manufacturers like Samsung to also keep certain "drivers" (software that controls your mobile's camera, mic, etc.). Imagine if home invaders had a key or code to be able to open your panic room. That would be disastrous! Well, today’s hackers have the keys to get into the Trust Zone! What is worse is that chipmakers and device manufacturers know that but can’t really fix it. How hackers got the keys to Trust Zone is really academic at this point, because it is what it is. Suffice it to say that the Operating Systems (OS) such as Android, Linux, and even Apple's IOS are to blame.

To better understand this mess the digital industry as a whole has gotten itself into, let’s take a brief stroll down memory lane. OS's were designed without thinking about security. Why? Because when they were built back in the 1960's no one really envisioned the digital world as it is today, with everyone on the planet being an active participant in it. The granddaddy of all the OS’s is Unix, which was developed by AT&T. From it come all the commercial OS’s we know and use today. Linux is a son of Unix, and it is the main OS which permeates everything commercially available in the world today. Everything! It is known as an "open source" OS, meaning that anyone can access its source code (some very smart people did some very stupid things and decided to forget about security thinking we would all hold hands and sing Kumbaya sharing technology and systems), and this is where the problem lies. Everyone in the world can have access to the foundation (source code) of the OS that controls everything we use today commercially and otherwise to a certain extent. Android, which is the standard OS in the majority (70+%) of mobile devices worldwide is in turn a son of Linux and grandson of Unix. Even IOS which runs all Apple mobile devices is compromised because it comes from a son of Unix called BSD 4.2. In fact, Apple's OSX, Windows, and pretty much every piece of software ever developed which we regularly use commercially is compromised and vulnerable because they all suffer from the same bad unsecure gene pool. This is why hackers have the keys to open all doors and systems. The deepening global crisis of corporate, governmental, and most recently individual cyber-attacks will NEVER end because we keep using Unix and all its open source derivatives.

There are other chip architectures out there which are not ARM-based, so they don't have Trust Zones, but they are also vulnerable through their Unix/Linux-based OS-IOS and Android.

You may think at this point that this doesn’t apply to you, and that your phone manufacturer is or will solve this. No, they won’t. Despite whatever they publicly state, internally they do not perceive their role as one to give you a

secure device vs providing you with a usable device that looks appealing for you to purchase and use. The common denominator across all mobile device manufacturers is their open source OS fraught with vulnerabilities that hackers know about and easily exploit. This is an openly documented fact. In essence- your phone calls, texts, emails, photographs, and data in general will NEVER be safe, pretty much anywhere, but especially on your mobile devices. It doesn't matter what you do.

In conclusion, all these so-called anti-viruses and mobile device management services are written to work on the same compromised OS and share the same vulnerabilities. Ultimately encryption is worthless. It doesn't matter who tells you what. Pretty dire state of events isn't it? Yes, and this is why the cyber-security problem is becoming epidemic. Is there a way out of this self-inflicted catastrophic predicament? Yes. We (humans) broke it, and we can fix it too, if we wanted to…

… at HIC we want to, we know how to, and we are doing it!

For the purpose of this memo I won't go into much detail on the factual information that backs up my statements, except to direct the reader to the National Vulnerability Database (NVD) published by the USA NIST (National Institute of Standards and Technology), which is a database of all the vulnerabilities in all the available commercial software, including operating systems. The salient point here is that OUR OS, known as "INTEGRITY™ 178B", has NOT been hacked in 20 years of being deployed and does NOT have a SINGLE vulnerability, being the only NSA (National Security Agency) EAL-6+ Level certified OS (secure and never hacked), when all other OS's (Windows, Unix, Linux, IOS, OSX, Android, VMWare) are certified at levels 4 and below (insecure and hacked continually since inception).

There is a second element with regards to securing a smartphone that is important. We do not need to simply guard against hacking-at-a-distance, but we also need to protect the phone itself from being stolen or used by people other than its rightful owner(s). Millions of valuable smartphones are stolen every year, and part of the motivation of thieves is that they could use the phones themselves or sell them to others. The most recent smartphone models are protected with some face and digital recognition, and access codes, but much has been written already on how these protections are not sophisticated enough. Biometric identification at the phone level is simply not advanced enough, nor thorough enough. But at HIC, as a successor company to many of my previous ventures in patented biometrics (including iris, fingerprint and voice), we have also incorporated this entire suite of innovations.

My vision is to create a completely secure mobile communications platform that can protect our voice communications, all data, cryptocurrencies, identity, our security and privacy, and ultimately enable complementary secure vertical applications and business, all on a recurring revenue-based secure telecommunications business model.

At HIC we protect people, their identities, all their data, transactions, and privacy-all enabled by a proprietary platform based on a uniquely secure smartphone that can't be hacked, which knows that you are you.

VISION BECOMES REALITY

The first part… was to design and build a truly secure smartphone, the Hoyos RISEN Smartphone. Early in 2017 HIC acquired a company formed by the former Motorola mobility senior team responsible for designing hundreds of models for Motorola that shipped hundreds of millions of devices over the last 20 years, representing

tens of billions of dollars in revenue. **At HIC we designed a smartphone utilizing an OS that is NOT open source, that has zero vulnerabilities, that according to the US and European governments has not had a single hack in the last 20+ years during its deployment in millions of systems, and which is used to protect the security of America's weapons arsenal**. It is called **INTEGRITY 178B**. HIC is the only company in the world with an exclusive long-term license from its owner, Santa Barbara-based Green Hills™ Software (GHS), to deploy it in mobile devices. At HIC, we took INTEGRITY 178B and combined it with Biometrics (multi-fingerprint technology created by me that performs instant capture with the rear camera of a smartphone, our own face, and the leading 3rd party voice) under the IEEE2410 protocol invented by me, our proprietary Hoyos RISEN Software Suite (for voice calls, messaging, and data security), and blockchain technology.

In one sentence: HIC is the ONLY phone run by an operating system that has NEVER been hacked and is impervious to hacking because it is not open source and has withstood the test of time. This is the same OS that has runs the USA's nuclear codes, bombers and fighter jets, among many other applications, for decades. But you may ask: can you run off-the-shelf apps such as WhatsApp without compromising the smartphone's security? Yes, in a way that does not affect the device's security in any way. A prior version of our secure smartphone, developed for the US military and in use in the battlefield, allows a specialist on the ground to call in secret bombing-run coordinates to his commander, yet subsequently use WhatsApp to call his/her loved ones back in the US. This holds for any Android app. This is achieved because Android is allowed to run on a secure "partition" above INTEGRITY; INTEGRITY runs the phone, and Android only runs the apps, but not the phone.

Moreover, the RISEN Smartphone can only be used by its registered owner(s), and when two RISEN Smartphones call each other, both users can be 100% certain that the person on the other line is who they say they are. And the RISEN Smartphone is sturdy, to prevent accidental damage, and made in the USA.

The second part…is to integrate the Hoyos RISEN Smartphone into a secure communication recurring revenue service model. This means that we sell a complete service on a multi-year contract that includes our secure smartphone, plus access to a cellular voice and data network. To do this we became an MVNO (Mobile Virtual Network Operator--such as TracFone, Boost Mobile, etc.). I hired the best guy in the business, who for the last 20 years was a senior executive for Sprint in the US and was responsible for setting up all their MVNO partners. In December 2017 we selected and signed T-Mobile as our network of choice, after having evaluated all operators in the US market. This effectively means that **we are also a telecommunications company**, capable of offering our enterprise and government clients, a unique secure communications service on a multi-year contract that includes our secure smartphone, plus access to one of the best cellular voice and data networks in the US. We are also applying this model internationally, where we will also deploy as an MVNO in a number of countries, and in others as a strategic revenue-sharing partner of local operators, as is the case prospectively with Deutsche Telekom for Germany and possibly other EU countries. The benefit to us of this business model is that it tracks the fast and highly profitable adoption cycles of the mobile telecommunications industry, which are very well known to operators and the capital markets.