QWYIT® LAB CYBERSECURITY BUSINESS PLAN

I. EXECUTIVE SUMMARY

Qwyit® LLC (dba “Qwyit® Lab”) is a cybersecurity engineering company that has developed disruptive and innovative cryptography that solves the continuous and multi-trillion dollar problem of cybercrime preying on the same vulnerabilities in today’s computer networks and devices. These vulnerabilities can be eliminated by **Authenticating and Encrypting Everything, Everywhere, Each and Every time**. No existing security protocol can do this; but Qwyit®’s authentication and encryption protocol is designed with the required and necessary properties to make this possible. Qwyit®’s protocol comprises blazing speed, elegant efficiency, infinite flexibility and mathematically provable security.

We seek investment to create the Qwyit® Lab – modelled after Dolby® Labs – in which we will create reference designs that incorporate Qwyit® cybersecurity protocols into existing products. We will demonstrate these reference designs to marketplace participants showing how they can achieve superior results in their own products, and then license Qwyit®’s technology to enable them to commercialize these new product versions.

Initially, we plan to concentrate on markets where security is nonexistent: *e.g.*, Internet of Things (IoT), Artificial Intelligence (AI), autonomous vehicle and others. This strategy seeks to avoid the “Standards Required” status quo: Qwyit® will leverage the emerging realization that 45 years of current methods remain inadequate. “*Companies will need to adapt as hackers evolve.*” Wash. Post, Feb. 22, 2021 The Cybercrime 202: Cybercrime skyrocketed as workplaces went virtual in 2020, new report finds.

We have a unique technology and a unique market position. We have outlined a unique *proven* and successful licensing model. Qwyit® has already built core software components that can be quickly integrated into devices to build demonstrations and proofs of concept. We have completed significant research and development efforts to build out the entire Qwyit® technology suite. We are seeking funding for the Qwyit® Lab, which investment funds will be used for: (i) customer acquisition; (ii) labor; (iii) Qwyit® Lab setup and operation; (iv) business development; and (v) demonstrations.

Qwyit® has the technology, the business model, the team and the solution to end cybercrime as we know it. With an investment of $3M, our financial projections estimate a 4th Year Profitability of about $30 Million. This represents a tenfold exit opportunity for a small $3M investment.

II. COMPANY SYNOPSIS

Organized in Virginia, Qwyit® LLC is a cybersecurity engineering company founded in 2014, but Qwyit’s principals have been working on security technology and unique cryptography since 1997. Qwyit is the sole owner of the patents and technology from these earlier efforts.

A. Technology:

1. Qwyit® Authentication and Data Encryption Protocol – simply the world's fastest authentication and encryption protocol
    - An elegantly simple digital stream cipher that provides embedded authentication and encryption for digital communications, assets and networks using a symmetric secret-key system and employing a federated trust model
    - Built on several distinct, innovative primitives leveraged in different and unique combinations to create perfectly secure authentication systems and ciphers
    - An endless variety of consumer products can be built from the Qwyit® Authentication and Data Encryption Protocol, such as encrypted phones, networks, devices, and hardware authentication and encryption chips; and these products can be built as reference designs in the Qwyit® Lab.
    - One cipher version of the Qwyit® Authentication and Data Encryption Protocol, called QCy™[1], is an idealized single clock cycle encrypt or decrypt capability providing continuous, mutual authentication and quantum safe encryption native within a chip.
2. 11 Patents Granted (10 U.S., 1 Japan), other patents remain pending:
    - Most recently, Qwyit® was awarded U.S. Patent No. 10,924,278 for its "*Authentication and Encryption Service Employing Unbreakable Encryption"* which issued February 16, 2021 (child patent pending) (this is the only patent to ever issue with "unbreakable encryption" in title or claims); and
    - U.S. Provisional Patent related to QCy™ filed in May 2020 (single clock cycle unbreakable cipher).
3. Two registered Trademarks
    - U.S. Trademark Registration No. 4,618,824 word mark QWYIT® for "Software development and product development in the field of secure communications"; and
    - U.S. Trademark Registration No. 4,618,852 design mark Q ® for "Design, development, and implementation of software for authentication and encryption."
4. A prolific writer and innovator, Paul McGough has authored over 40 White Papers describing various aspects of our technology, a wide variety of applications, and potential markets.
5. Core Software modules have been built and tested to implement various aspects of the technology, such as test vectors, timing simulations, testing, primitives, SDKs, and modules for use in software and hardware description languages.
6. "Extraordinary claims should require extraordinary evidence to be believed." - Kevin Kelly
    - Qwyit® built three working chip demos using different FPGAs and key sizes (Intel Arria V and Stratix V (using 256-1024 bit keys), and Achronix Speedster 7T (using a 256-bit key) providing verification of our claims: 256-bit (up to 1024-bit) encryption in 1 clock cycle (speeds up to 300 MHz., or 154 Gb/s); decryption works in single clock cycle as well, and nothing can be faster than one clock cycle!

[1] Patent Pending

- Online demo shows HDMI video being encrypted and decrypted on an Arria V FPGA development kit exhibiting no latency when comparing original HDMI video and the same video being encrypted and decrypted.
- Multiple travel demo kits have been built to permit our sales team to demonstrate these in person to potential customers.
- Complete, multiple independent reviews provide assurance that our technology delivers our claims and specifications. Academic experts are available to discuss the cryptographic foundation of Qwyit®'s Perfect Secrecy claims.
- Our methods are based entirely on fundamentally sound mathematics and cryptographic principles; while still being entirely innovative and foundationally scientifically unique.
- Transparency is our tenet. Everything we do, the ways we do it and the results we have achieved are available and independently verifiable.

B. Existing Technology Components Ready for Implementation in Reference Systems

1. Hardware: QwyitChip™ FPGA architecture, existing versions:
    - Intel Arria V
    - Intel Stratix V
    - Achronix Speedster 7T
    - Code available in Verilog and VHDL
2. Software: QwyitSDK™ available in multiple versions: e.g., C, C++, Java
3. Authentication Key Management: QwyitKey™ prototype-ready for cloud based implementation.
4. Qwyit has been implemented in the following products:
    - Ethernet radios were converted to Qwyit enabled radios in 8 weeks; full Qwyit communication was added via software update
    - Qwyit's cipher was added to Open VPN in 5 man days to enable Qwyit to be selected as a desired encryption
    - Qwyit was built into an FPGA in 8 weeks.

C. Qwyit® Potential Products Services

1. QwyitKey – Participant managed, independent-trust authentication service for secure messaging.
2. QwyitChip – Qwyit® authentication and encryption protocol on an integrated circuit chip, such as an FPGA, CPU, ASIC, GPU and SOC.
3. QCy (QwyitCipher) – Fast Unbreakable Cipher optimized for hardware implementation, built in Verilog and VHDL; PDAF-SEC Cipher.
4. QwyitFone -- Qwyit® authentication and encryption protocol in a mobile phone.
5. QwyitSDK – Qwyit® authentication and encryption protocol in a single SDK library (identical to QwyitChip but in software, C, C++, Java).
6. QwyitTalk – cloud Qwyit® platform: Security As A Service – Any app can simply attach, use the service, and provide provably secure communication, replacement for transport layer security (TLS)

7. QwyitStore – Storage solution employing Qwyit® authentication and encryption protocol that enables real time control of participant data when stored on third party platforms.
8. QwyitCard – Qwyit® method to provide superior security on a credit card, for a credit card transaction. QwyitCard can be performed on an 'old magnetic stripe card', faster, and with more security properties, e.g., no fraud, no card replication.
9. QwyitCash – This is tomorrow's solution to the entirety of retail credit transactions – no cards, no readers, buy wherever, whenever.

D. Potential Markets:

1. IoT devices – nothing exists capable of providing authentication/encryption for all types of IoT devices, including small, low power devices;
2. AI – nothing exists that can withstand attacks by Artificial Intelligence;
3. Autonomous vehicles – nothing exists that can provide systematic protection for all systems in these vehicles;
4. Mobile phones – no cellular phones employ end to end encryption through the cellular channel;
5. Storage – existing encryption is too cumbersome and slow to suit high speed, big data storage systems;
6. Health computers and networks are requiring more and more data protection and are huge targets for ransomware;
7. Government systems require higher security which currently requires an endless increase in key size -- Qwyit® Authentication and Data Encryption Protocol need not increase code word size to provide increased security.

E. Value Proposition Basis

In 2021, Global Semiconductor Industry sales are projected to be $460 Billion and Global Cybersecurity products and services are projected to be $1 Trillion. A modest 10 year 25% penetration would yield $358.25 Billion. Our financial projections estimate a 4th Year Profitability of about $30 Million. This represents a tenfold exit opportunity for a small $3M investment. See appendix for further details. Beyond this, once Qwyit's protocol becomes approved by the U.S. government, Qwyit's revenue ceiling is extremely high.

III. CYBERSECURITY PROBLEM SOLVED BY QWYIT®

Without a Universal Security Process, cybercrime will continue. The successful attacks reported in the media form the tip of the iceberg (e.g., Equifax – 143 Million records stolen, SolarWinds/Russians – almost every Government Agency broken into). Despite using only government approved protocols, these attacks continue to be successful. Cybercriminal activity is one of the biggest challenges that commercial entities will face in the next two decades. Cybercrime is the greatest threat to every company in the world. Cybersecurity Ventures predicts cybercrime will cost the world in excess of $6 trillion annually by 2021, up from $3 trillion in 2015. – From Cybersecurity Ventures 2020 consensus

The question is: Do you think we need new security tools, or do we need the current tools in more places?

Current Transport Security Layer (TLS) Version 1.3, the Gold Standard for security "Best Practices" comprises three distinct algorithms, which requires at least five transmissions between participants. These include an asymmetric key exchange, a digital signature, and symmetric encryption, *e.g.*, ECDHE-RSA-AES256. ECDHE (Elliptic Curve Diffie Hellman) was invented in 1976. RSA (Rivest, Shamir, Adleman Prime Number Factoring) was invented in 1977. AES (Advanced Encryption Algorithm) invented in 1999 became US Government Standard in 2001.

For 45 years, security implementations have not changed. Current security measures cannot solve three agreed-upon problems:

1. Existing measures are not quantum safe; all existing measures, except ours, will be completely vulnerable within 5-15 years. Key size will continue to need to be increased just to remain ahead of increasing computer power, at the expense of network computing performance.
2. None of the existing cybersecurity protocols fit in today's hardware devices for networks, storage systems, or other computing devices (e.g., FPGAs, CPUs, GPUs, SOCs). While AES has been built in hardware as an extension available to other hardware devices, AES is not capable of being native within any processor chips that perform other communication functions. Requiring the data to be output from one chip to another to be encrypted and then returned to the original chip provides an inherent limitation in performance.
3. Existing cybersecurity systems are a limiting factor for tomorrow's systems. For existing cybersecurity, computing remains extremely slow, code size is large and becoming larger, huge bandwidth is required, and documentation and implementation is overly complex. The learning curves for new engineers tasked with adding encryption to their applications is significant. These performance hits remain true with today's key sizes. The larger key sizes of tomorrow will grind most networks to a halt.

Are these limiting problems the reason for the Cybercrime? The answer does not matter because if they are, why keep using them; and if they are not, having had 45 years to put them everywhere, why are not they used everywhere? Is not 45 years long enough to know <u>we need new security tools?</u>

Since it is not possible to solve the Cybercrime problem using the current methods, what would the methods look like that can solve the problem?

Cybersecurity Features to Solve Today's Problems	**Cybersecurity Solution:** Qwyit®
A simple examination of the three problems with today's security protocols results in the conclusions below.	The Qwyit® Authentication and Data Encryption protocol is designed with the required properties to stop Cybercrime. Qwyit® integrates true Perfect Secrecy which completely eliminates entire classes of attacks on encrypted data. Qwyit® implements

	mutual continuous authentication in every data interaction, which stops unauthorized access.
Any Security Protocol must be Quantum Safe, which we define in the broadest sense. The protocol should not be dependent upon the computational capability of the attacker, i.e., the protocol should not be computationally bound. Regardless of how powerful computing becomes, security algorithms should still work to secure the data, because there will be always be the next super computer after Quantum Computing. Such capability is defined by Shannon as "Perfectly Secret", there is no way to compute the single, correct answer ever.	Qwyit® Authentication and Data Encryption provides embedded authentication and data security in a stream cipher for digital communications, assets and networks using a symmetric secret-key system and a federated trust model. Qwyit's protocol is built on several distinct, and innovative primitives. In different and unique combinations, these primitives create perfectly secure authentication systems and ciphers. Qwyit's ciphers result in under-determined equations sets, thereby ensuring they are not computationally bound. Qwyit's authentication and encryption protocols satisfy Shannon's Perfectly Secret requirement. No amount of computer processing can compute the single, correct answer ever.
Any security protocol must exist in hardware – if data security remains at the mercy of OSI software layer solutions, whatever solution is proposed will always be vulnerable to attack: the fundamental difference between residing in hardware and software is the inability to access the security in a chip.	QCy™ provides an idealized single clock cycle encryption cipher with embedded continuous, mutual authentication and quantum safe encryption in every instance, which is optimized for hardware implementation.
Any security protocol must be Fast, Efficient, Flexible and Simple – 45 years have shown that speed, bandwidth, code size, flexibility and simplicity in implementation are critical to widespread use. Without these properties, engineers will continue to opt for little or no security given the performance loss.	QCy™ works within every system's inherent data processing; it fits within any system's architecture; it performs authentication and encryption within any process; and it will work perfectly for eternity. Imagine the end of encryption upgrades.
Speed Requirement – to be used all the time and everywhere, a security protocol should operate as if it was not there, i.e., within the latency of the device, storage, transmission, or any OSI layer processing. When faced with choosing to implement encryption or not, an engineer will opt for the encryption if the performance does not change.	***Speed*** – QCy™ operates in a single clock cycle for either encryption or decryption with embedded authentication on every 256-bits employing a unique key for each 256 bits. Performance has been shown to be equivalent for 1024 bit operation as well. QCy™ has been benchmarked on several FPGA's, such as the Intel Arria V, the Intel Stratix V and the Achronix Speedster 7T. Each time QCy™ achieves this performance. Nothing can ever be faster than QCy™ because nothing can be faster than one clock cycle.

Efficiency Requirement – To be systemically effective, security should exist in every hardware device, or software controller. There should be no bandwidth degradation, or significant impact on code size.	***Efficiency*** – QCy™ has been built in a highly efficient design to maintain a tiny footprint in code for either hardware or software implementations. QCy™ has been implemented in less than 300 lines of code in VHDL and less than 10 KB in software. QCy™ has no bandwidth expansion or performance degradation. QCy™ has been built in several languages, Verilog, VHDL, C, C++, and Java and can be easily ported to every development platform. QCy™ does not increase the bandwidth of the underlying data
Flexibility Requirement – The technology must be adaptable to different implementations or environments.	***Flexibility*** – QCy™ has been designed to work in any platform or device using any trust model, with mutual continuous authentication and encryption. QCy™ can be easily modified to work in any configuration and design without loss of security.
Security – The security must be Perfectly Secret, e.g., quantum safe.	***Security*** – QCy™ protocol meets Shannon's defined Perfect Secrecy in an ideal system.
The Security must authenticate and encrypt everything, everywhere, each and every time.	QCy™ authenticates and encrypts every use, fits everywhere and can be used each and every time.

IV. CYBERSECURITY ANSWER: QWYIT™ PROLIFERATION

Current digital security's proliferation was a gradual process and changing that security will be too. There are a few key parameters to be aware of during any security upgrade, including a Qwyit® technology revolution.

1. True innovative security can be immediately implemented where none exists. The market for this is immense, in desperate need – and will likely fail in the future without it. Most of these areas are lacking because current methods do not fit, work, or apply. Qwyit® has the demanded properties of speed, efficiency, flexibility and future assurance to succeed.

2. As there are "Best Practices" required in several areas, such as finance and government, Qwyit® will not initially focus on places where standards already exist. After Qwyit® has taken hold in other areas, and demonstrated superior performance, then Qwyit® will work to have the "Standards" rewritten to include its technology. This is a time-consuming process, so these areas will follow innovation disruption. But the potential profit is massive once approved.

3. As proliferation increase, existing technology pieces can be leveraged such that parts of the new technology can be swapped out with some of the worst limiting old technology parts – implementing superior "bridge solutions" that eventually will be completely replaced with all new technology. In security, this means that current PKI authentication systems can be leveraged for key creation, distribution and management while swapping out the encryption. In the Qwyit® protocol, this means initially swapping out AES for QCy™ because the key requirements are identical.

4. As routine maintenance and system updates occur, the complete solution can then be delivered. In the Qwyit® protocol, this means exchanging one of our Authentication key management solutions for PKI:
    - QwyitTalk™ -- comprises a direct, identical process replacement using Qwyit®'s superior primitives; and/or
    - QwyitKey™ -- comprises a future-demanded Anonymous Authentication Service, the world's first participant-managed, independent-trust authentication service.

V. BUSINESS MODEL – QWYIT® LAB

These topics are grouped together because of our unique technology and market circumstances. We are a cybersecurity component; a completely new and fundamentally different (and superior) authentication and encryption protocol – one designed from core principles with expert innovation. Qwyit®'s protocol fits into the entire digital architecture: devices, networks, data stores, the cloud…everywhere. Those are all operated, produced, managed, owned and used by a wide range of entities – all of which can benefit from Qwyit®'s technology; they can all be customers in multiple ways.

All this diverse potential results in difficulty in defining our company. The main question is: How do we monetize our superior security technology? Fortunately, one does have to "reinvent the business wheel" to solve this problem. Prior success solving a similar business problem exists. Ray Dolby succeeded in creating an $8 Billion company called Dolby® Labs:

- Based on superior technology
- Building prototypes integrating his audio technology into existing and new products
- Demonstrating those products to marketplace companies, and obtaining their buy-in
- Licensing the superior technology to them to build the market products.
- Dolby® Labs is a tremendous success story, profiting from those marketplace producers.
- Today, Dolby®'s technology can be found in almost every audio product.

Qwyit® will build reference designs and prototypes – taking existing products and replicating their current and future uses while adding Qwyit®'s no degradation cybersecurity. We will hold 'Demo Days' for prospects to view their current products and systems integrated with quantum safe cybersecurity working exactly as they do insecurely. Just as it was for Dolby®'s prospects hearing clear sound for the first time, Qwyit® will demonstrate secure products that perform identically to nonsecure versions. As security is a demanded capability, we are confident that license sale revenue will result. Qwyit envisions creating reference designs in 1-3 months, thereby enabling demonstrations within about 3-4 months from funding.

A. First Reference Design -- IoT

Our 1st Reference System will be in one of the largest growing technology marketplaces: IoT. "The global IoT market is expected to reach a value of $1,386.06 billion by 2026 from $761.4 billion in 2020 at a compound annual growth rate of 10.53%, during the period 2021-2026." There is only one major market restraint: "Issues Related to Security and Privacy of Data and Connectivity of Devices and Interoperability." Solve those, and market capture is guaranteed.

IoT – As an example, implantable medical devices are known to be vulnerable to external attack. The experts have developed over 40 communication and data protocols, yet none of these provide end-to-end security for such small, low powered devices. There will be over 25 billion devices in 2025. The security concern is the biggest challenge in IoT.

Fortunately, it is not hard to envision the solution: secure every device (no matter how low powered or computationally constrained) with embedded authentication and encryption in the chipset, and control hubs owning any network connectivity. Using Qwyit®'s security protocol, end-to-end is assured with no performance degradation. No other way exists to improve the current ill-suited, and flawed security complexity.

There cannot be a better first market Reference System end-to-end security implementation demonstration to open the Qwyit® Lab. Here's the process that we will repeat over and over in various, well-qualified market voids, for IoT product Reference System developments and sales.

B. Qwyit Lab Process:

1. *Pick a market*: *e.g.*, *IoT*

2. *Pick a product*: Choose a well-known, security-hampered yet security-demanded medical device, such as a pacemaker: Villains in television shows *The Americans* and *Homeland* assassinated American Vice Presidents by hacking their pacemakers.

3. *Obtain current versions*: Acquire and replicate a complete medical IoT framework to demonstrate Qwyit™ security, such as a pacemaker, server and software control application in a hospital network – a Reference System of an end-to-end device-to-server-to-service-to-hospital architecture.

4. *Develop Reference System:* Build Qwyit®'s cipher directly into the framework in all applicable and essential locations. We will demonstrate true end-to-end quantum safe, fast, efficient, mutually authenticated and encrypted traffic and data storage. We will replicate and operate usual control application software, showing no degradation, complete end-to-end security – and differentiate what we have accomplished within current capability. We will do this in as

many demonstrable ways possible: in the actual opened firmware (if available, otherwise replicated), in the performance metrics, in the traffic analysis, displaying it, providing papers documenting it – all with clear depictions of where, how much, how often we have improved the entire end-to-end security all within the same operating metrics as current insecure traffic. The same way Dolby showed crystal clear sound in his first tape recording units that instantly, vastly changed the quality of recorded sound, Qwyit® will show encrypted data handling that will instantly, vastly forever change the way IoT data is processed: end-to-end authenticated and encrypted without any latency difference, user complexity, or bloated infrastructure and bandwidth penalties.

5. *Hold Demonstration Day*: Inviting representatives from all possible IoT medical device manufacturers, service application developers, medical consulting practices for word-of-mouth marketing, hospital IT staffs – any responsible participant in the health and medical devices area. And any and all general IoT responsible parties to which we can demonstrate cross-product applications, and with which we can develop partnerships for their products and services. This list is never exhausted; and 'Demo Day' can be both a pre-determined *event*, as well as an any-day occurrence.

Our Qwyit® technology base has all of the required science properties, user simplicity and business model effortlessness to succeed exactly like Dolby.®

C. Additional Products for Development in the Qwyit® Lab

1. Qwyit® Fone

We will take an open source mobile phone operating system and integrate our Qwyit® protocol into various features of the phone, particularly the cellular calling capability. The phone will be used to obtain keys from our QwyitKey cloud server and then make encrypted calls to other Qwyit® enabled cell phones. The QwyitKey cloud server lies at the heart of a participant managed key distribution system. No one but the actual user knows its keys. The QwyitKey server merely facilitates key creation and connection of users between and among each other. Using the cellular channel distinguishes Qwyit® from other technology that uses VoIP technology for calls that are allegedly encrypted but only once the call reaches the network, such as WhatsApp and TextPlus. Qwyit Fone is unique in that the keys are managed by the participants and the encryption is end-to-end. No one but the users can know what the keys being used are and therefore complete independence from outside intervention and manipulation.

2. Government Approved Security

One additional product being worked on in the Qwyit® Lab will be leveraging our technology to obtain government approval of Qwyit®'s security protocol for use in systems requiring government approved encryption. This effort requires a full-time engineer/business development person to manage the process of obtaining government approval. This process takes about 3 years, but the potential payoff is huge. Once approved, the Qwyit® protocol will have few competitors and many opportunities for licenses.

3. Qwyit Enabled Secure Networks

Qwyit® has new technology to be announced once its patent is filed relating to secure networks. This technology will be featured in one of the reference designs in the Qwyit® Lab.

D. New Inventions and Innovation

Qwyit® will continue to innovate and provide ground-breaking technology through its efforts in the Qwyit® Lab.

VI. COMPETITION – THE STATUS QUO AND BEYOND

Security is 'expert' stuff. Experts already know everything. There is not much room to maneuver, and that is the definition of the status quo. The status quo is filled with leaders, experts, followers, and users who present three serious issues:

1. They protect the current stuff.
2. They cannot see how or why anything else is needed or ever will be.
3. They most certainly cannot visualize the future because these individuals are consumed with the present

We are going to avoid the status quo as we have outlined in our proliferation strategy and as we go about our Qwyit® Lab operations, we expect to encounter the protectors of the status quo. Our mission will remain to concentrate and operate in those places where current security is either nonexistent (e.g., AI, Autonomous Cars), or seriously lacking (IoT, entertainment, mobile). But there's more to the security landscape than the status quo:

Those nonexistent areas are brand new technology frontiers. And luckily, we do not have to invent new technology frontiers along with our component security technology; all we need to do is properly present it to those existing frontiers – and as we succeed and gain traction, newly invented frontiers will seek us out to include our tech into their initial designs.

VII. QWYIT® TEAM

R. Paul McGough – Founder, Inventor, acting CTO and Chief Scientist

Paul McGough is a telecommunications expert with over 35 years of progressively responsible experience managing IT technology teams for the development, integration, implementation and support of financial, project management, database applications and security systems. In these 35 years, Paul has been an inventor, and entrepreneur while holding senior positions with AOL, CSC and SAIC, including 10 years as a program manager of highly classified government secure communications and software engineering developments. Mr. McGough co-founded Qwyit® where he remains acting CTO, Chief Scientist, and Qwyit® inventor, and author.

Michael P. Fortkort, Esq. - Co-Founder, *Chief Executive Officer and General Counsel*.
Mr. Fortkort is a registered patent attorney and technology lawyer who worked with technology startups for over 30 years. A Georgetown University Law Center graduate (*cum laude*), Mr. Fortkort spent ten years with a large Intellectual Property Law firm, then founded his own boutique IP firm. He is currently *of counsel* to Protorae Law PLLC, a business law firm. Prior to entering the legal field, Mr. Fortkort worked for seven years as an engineer for the U.S. government on classified communication related developments. He received a B.S.E.E. from the University of Notre Dame and an M.S.E.E. in Communications from George Washington University. Mr. Fortkort worked on patents for the technology now known as Qwyit® with Paul McGough starting in 1998 and co-founded Qwyit® with McGough in 2014. Mr. Fortkort helped write the core functions in Verilog used in the Qwyit® FPGAs and in C in the Qwyit® SDK. An active entrepreneur, Mr. Fortkort also founded a transportation company (Chariots For Hire) in Washington, D.C. in 2002 which is now the 4th largest in the region. He currently serves as its President and Chairman of the Board.

Travis Lowe - Senior Hardware Engineer
Mr. Lowe is an experienced electrical engineer with a strong background and training in the design, analysis, inspection, testing, troubleshooting, and repair of electronic systems. He utilizes in-depth and extensive knowledge and experience in designing and maintaining multiple electromechanical systems. He provides exceptional multi-tasking and organizational skills; adeptly managing multiple projects while ensuring high rates of productivity. Travis worked at General Dynamics, L-3 Technologies, MOOG-Protokraft, Peco-Inspx, etc. Mr. Lowe developed the Qwyit® FPGAs and the demonstration kits showing single clock cycle encryption of HDMI video.

Sudhakar Kamma - Senior Software Engineer
Mr. Kamma has 20+ years of total experience in design and development of Java full stack (J2EE, Spring framework, Hibernate, Server side, GUI, Messaging), C++ real time and Web based applications. He is AWS Certified. Sudhakar has worked with Leidos (for FAA ERAM project), several financial firms (SWIFT, CLS Bank, Interactive Data, McGraw-Hill Financials, Citi Group, Credit Suisse, Norwest Financials, SWIFT, Western Union), in telecom (AT&T, Verizon, Avaya), insurance (MetLife) and government (State of New Mexico). Mr. Kamma wrote the Qwyit® SDKs in C, C++ and Java and developed the QwyitTalk and QwyitKey client/server applications.

Charan Kaur – System Architect and Database Specialist
Ms. Kaur has wide experience working with Oracle and Sybase database systems. She has worked built the cloud server for Qwyit and manages Qwyit's AWS servers.

Taylor McGough – Cryptographic Engineer
Mr. McGough earned his masters' degree in computer science from Virginia Tech and his BSEE also from Virginia Tech. Versatile in a large number of computer languages, Mr. McGough has written key portions of the Qwyit code in our ethernet radios proof of concept and our FPGAs.

As outlined in our financial appendix, Qwyit® will add business development support for Qwyit® Lab product research, selection, partner acquisition, prospect demonstrations, and additional engineering support for web platform staging (QwyitTalk™/QwyitKey™), Database management, and authentication management.

VIII. FUNDING AND FINANCIALS

We have a unique technology and a unique market position. We have outlined a proven licensing business model to deliver success. We have completed all research and development efforts for the entire Qwyit™ technology suite – all new funding is to be used for Qwyit® Lab go-to-market and customer acquisition. We know what we have accomplished thus far, and what it took to produce: We have delivered two FPGA demos and acquired access to our starting technology and sales teams for $160k – with all executive management, technical design and direction performed for free.

Qwyit® is looking for $3M investment for 30% equity. Investment funds would be used for labor, Qwyit® Lab setup and operation and business development, and Demo-Day cycling. An investor could exit in Year 4 with a 10x return.

Current Capitalization		
Member	**Capital Investment**	**Share**
Paul McGough	$1,000,000	65%
Michael Fortkort	$200,000	35%
Convertible Notes	$160,000	TBD
Total	$1,360,000	100%

Investment Capitalization		
Member	**Capital Investment**	**Share**
Paul McGough	$1,000,000	40.8634%
Michael Fortkort	$200,000	22.0033%
Convertible Notes	$160,000	2.1333%
Investor to be named later	$3,000,000	30%
Option/Vesting Pool	$0	5%
Total	$4,360,000	100%

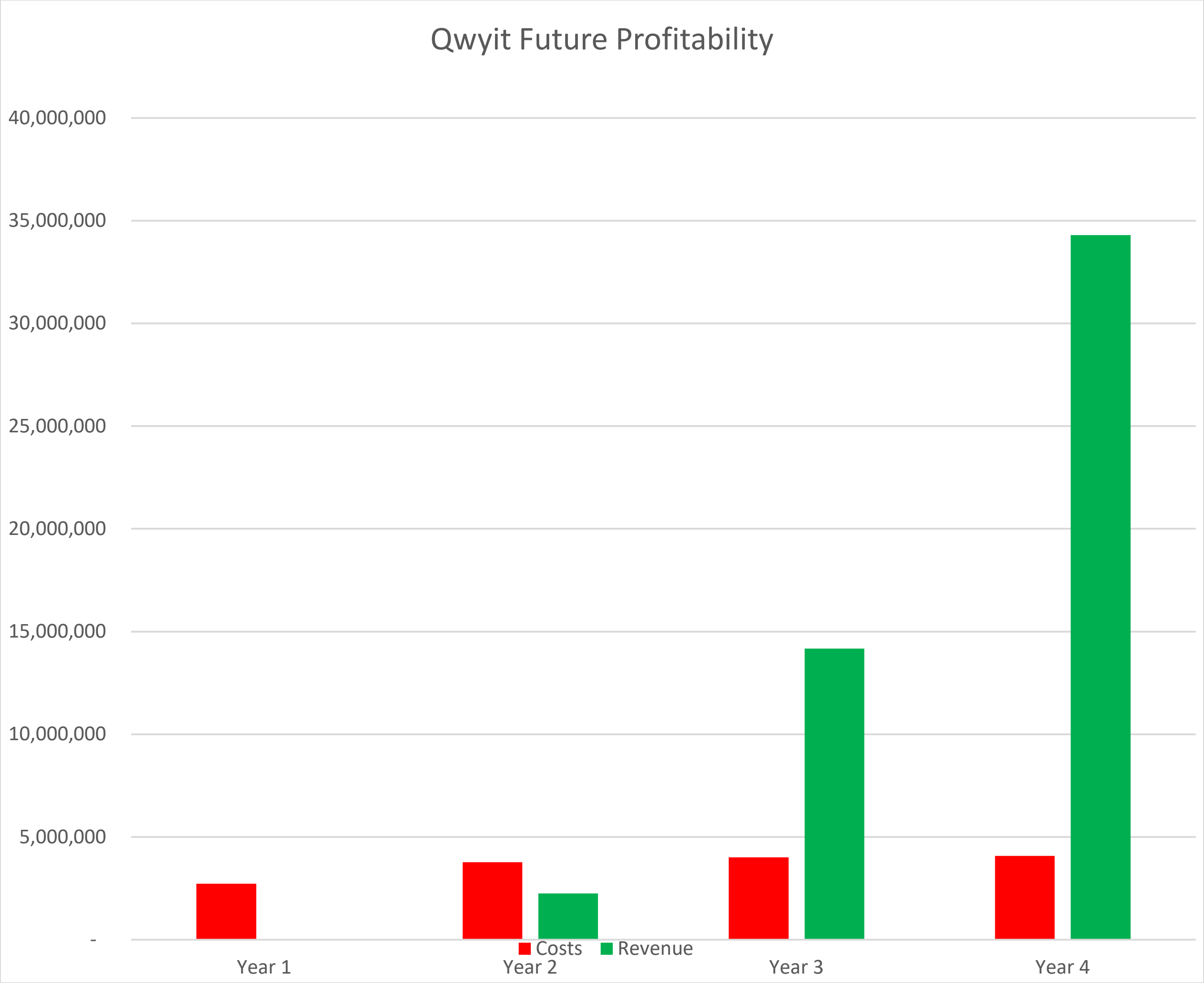
Qwyit® expects to require a 12 month burn rate from funding to 1st license. Projections begin at month 12, initial profitability at end of Year 3. $3M is a reasonable investment with reasonable fund management, giving us a 12-month uninterrupted setup and execution of the Qwyit® Lab. We will provide 2-3 prototypes, 3 Demo Days (figuratively) for a minimum of 25 market prospects. The worst we will do is 2-3 licenses; we are confident we will do better. Financial Details in Appendix.

Qwyit® License Types **General IT licensing – including an upfront payment of 20-30%, basis, maintenance, etc.**	**Examples**	**Price**

Full: Complete corporate entity, for any application or area (one per entity)	Cisco, Softeq, Intel, Dell, Quantum	$1 Million+
Product: Product-based, specific corporate, product or application (one or more per entity)	Samsung Galaxy S1, Google Nest, Ring	$1 – $1M
Time of Use: Time-based, specific corporate product, area or application (one or more per entity)	AWS, Snowflake, UiPath	~$1,000+ per month
Educational or Personal: Research and personal product or application (one per entity)	Stanford, MIT, John Doe, Jane Doe	$1 or free

2nd Year Licensing revenue projections ($2.23M):			
Year	**Type**	**Number**	**Income per month**
2	Full	1	$83,000 ($1M/year)
2	Product	4	$33,200 =$8300 each ($100,000/year)
2	Time of Use	1	$75,000
Total			**$191,200 ($2.294M/year)**

Years 3, 4 are an ever increasing mix of all License Types:



IX. Conclusion

Qwyit® is a unique opportunity with huge potential upside. Qwyit has a knowledgeable, experienced team and vetted, complete technology. Employing a proven go-to-market business model for the unique circumstances, Qwyit® is well positioned for success. The market potential remains wide and growing with new technology frontier opportunities – and with no legitimate security competition. Simply put, the status quo cannot bridge the technology chasm, but Qwyit® can.

Appendix – Financial Detailed Spreadsheet

Financial Projections

	Year 1	Year 2	Year 3	Year 4
Revenue				
Licensing - Full	$ -	$ 1,000,000	$ 10,000,000	$23,000,000
Licensing - Product	$ -	$ 350,000	$ 1,550,000	$ 4,925,000
Licensing - Time of Use	$ -	$ 900,000	$ 2,625,000	$ 6,375,000
Total Revenue	$ -	$ 2,250,000	$ 14,175,000	$34,300,000
Salaries and Benefits				
Chief Executive Officer	$ 225,000	$ 225,000	$ 225,000	$ 225,000
Chief Scientist	$ 225,000	$ 225,000	$ 225,000	$ 225,000
Chief Technology Officer	$ 225,000	$ 225,000	$ 225,000	$ 225,000
Executive VP, Business Development	$ 200,000	$ 200,000	$ 200,000	$ 200,000
Manager Level Business Development	$ 100,000	$ 100,000	$ 100,000	$ 100,000
Senior Hardware Engineer	$ 175,000	$ 175,000	$ 175,000	$ 175,000
Senior Software Engineer	$ 175,000	$ 175,000	$ 175,000	$ 175,000
Engineer 1 - Medical Device sector	$ 175,000	$ 175,000	$ 175,000	$ 175,000
Engineer 2 - Telephone sector	$ 175,000	$ 175,000	$ 175,000	$ 175,000
Engineer 3 - Government Security sector	$ 150,000	$ 150,000	$ 150,000	$ 150,000
Cryptography Expert - part time academic	$ 50,000	$ 50,000	$ 50,000	$ 50,000
Chief Financial Officer - fractional first 12 months	$ 87,500	$ 175,000	$ 175,000	$ 175,000
Accountant: hands-on senior - delayed start	$ 40,000	$ 80,000	$ 80,000	$ 80,000
Clerical/Administrative - 1	$ 40,000	$ 40,000	$ 40,000	$ 40,000
Clerical/Administrative - 2 - delayed start	$ -	$ 60,000	$ 60,000	$ 60,000
Human Resources Manager - fractional first 12 months	$ 87,500	$ 175,000	$ 175,000	$ 175,000
Human Resources/Recruiting generalist - delayed start	$ -	$ 85,000	$ 85,000	$ 85,000
Subtotal, Salaries	$ 2,130,000	$ 2,490,000	$ 2,490,000	$ 2,490,000
Benefits and Other Direct HR costs				
FICA taxes - FICA limit $142,800 for 2021	$ 132,060	$ 154,380	$ 154,380	$ 154,380
Medicare taxes	$ 30,885	$ 36,105	$ 36,105	$ 36,105
Health Insurance	$ 108,000	$ 118,800	$ 130,680	$ 143,748
Worker's Compensation premiums	$ 5,400	$ 5,400	$ 5,400	$ 5,400
401(k) Match - assuming 3%; highly comped have match limits	$ 63,900	$ 63,900	$ 63,900	$ 63,900
Commissions - payouts beginning in year 2 to be based on number of contracts closed and other factors	$ -	$ 319,500	$ 498,000	$ 498,000
Stock Options (placeholder for discussion; non-cash expense)	$ -	$ -	$ -	$ -
Subtotal, Benefits and Other Direct HR costs	$ 340,245	$ 698,085	$ 888,465	$ 901,533
Total Salaries and Benefits	$ 2,470,245	$ 3,188,085	$ 3,378,465	$ 3,391,533
Selling, General and Administrative Expenses				
Rent (remote for first 12 months, maybe longer)	$ -	300,000	315,000	330,750
Building parking, security other items not in base rent	$ -	9,450	9,923	10,419
Internal software, licensed (Accounting, CRM, Docusign, etc)	$ 30,000	31,500	33,075	34,729
Internal hardware/laptops	$ 30,000	10,000	10,000	10,000
Telephone (reimb for cell phones and/or telecommunications)	$ 6,000	12,000	12,000	12,000
Dues & Memberships to Cyber Professional Organizations, etc	$ 6,000	10,000	12,000	12,000
Marketing, Sponsorships, website development, etc.	$ 60,000	72,000	86,400	103,680
Publicity	$ 12,000	14,400	17,280	20,736
Legal services	$ 50,000	60,000	72,000	86,400
Tax preparation services	$ -	6,000	6,600	7,260
Payroll and 401(k) processing fees	$ 6,000	6,000	6,000	6,000
Recruiting advertising	$ 6,000	6,000	6,000	6,000
Travel and/or webinar development	$ 30,000	30,000	30,000	30,000
Directors and Officers Insurance	$ 15,000	15,000	15,000	15,000
Property Insurance	$ -	750	750	750
Total Selling, General and Admin Expenses	$ 251,000	$ 583,100	$ 632,028	$ 685,723
Total Expenses	2,721,245	$ 3,771,185	$ 4,010,493	$ 4,077,256
Net Profit (Loss)	(2,721,245)	$ (1,521,185)	$ 10,164,508	$30,222,744