The multilayered biometric security system serves the purpose of enhancing the security measures taken today. It will act as a defense against the unwanted additional wall of defense against unwanted intrusions of hackers and attackers with malicious intent. The product would be composed of multiple biometric systems working together to increase an entity, or system's, security defenses. Some of the biometrics include digital signatures and typing rhythm. When the biometrics are combined, they provide layers of defense with the goal of making it less likely for an intruder to gain unauthorized access. It would do so by conducting security checks to ensure the person requesting access is authorized. Otherwise, it will deny the user. The subtopic is adapting different means of protection to strengthen a system's defenses. A couple of keywords used to describe the technical area this product relates to are cyber security, biometrics, machine learning, security breach, security infrastructure, and intrusion defense.

This Small Business Innovation Research Phase I project will provide a great deal of technical challenges and difficulties in order to make it an effectively working system. Some of the technical hurdles include attaining the correct, physical biometric systems for the project, correctly coding the system to recognize different voice frequencies, brainstorming a way to differentiate the different keystroke rhythms people possess, and one of the biggest challenges, combining them all to work together seamlessly. If the challenges are met and overcome, the result will be a product capable of providing a high level of security to whatever it is implemented on. In addition to the security functions, it alleviates some of the stress on both internal and external stakeholders, as the system works to increase security measures, and reduce the possibilities of intrusion. In order to reach the aforementioned goals, it is crucial to search for the necessary parts, carry out a great deal of research to find the right code and implement it, and conduct trials to determine the best combination for the various pieces.

Not only could this security system improve and increase the number of defenses utilized today, it would also help ensure the safety of sensitive information. No security system is perfect, but this security systems provides a great deal of protection as it implements numerous methods of security seen today, but in a more efficient manner. This security system would help meet company needs for protection, improve the service provided to customers, and most importantly, save a great deal of revenue for the company which would be spent on recovering from a cyber attack. The benefits mentioned would translate to companies being able to utilize their saved funds to provide more for their customers, including additional security packages and more efficient features for the service they provide. The overall gain would lead to an increase in stocks, and a more successful company. No longer will they have to fear their business being the next on the news for a security breach. Rather, it will be praise for the dominance they would now have in the market.

Elevator Pitch

Have you heard the news of the different entities experiencing security breaches, which have ultimately led to a critical financial loss? Did you know each of them believed they were completely protected since they had passed the security check, which, in reality, is just checking off a box stating they have some form of security? Do you want to be next? If not, then this multilayered biometric security system is just the tool you need.

The product is meant for organizations, companies, and businesses - public, private, nonprofit, and more - to be able to provide more secure, efficient, and reliable security measures to its customers. Typical systems tend to have one line of defense and they have yet to be truly tested for security holes and/or isn't as extensive as it should be. This system will significantly increase your company's security hygiene, and ensure you are much less likely to get breached. With all the incidents being announced on various forms of social media in regards to cyber security, people are hesitant and unsure of who to trust. If you adopt, and implement this system, you can guarantee your customer's safety, which in turn, will build trust.

When you encounter a customer, some of the many concerns they will vocalize is how secure your systems are, and what security measures have you taken to ensure their information is not susceptible to falling into the wrong hands. The more security-conscious individuals will take it a step further, and ask how often your security is updated, or checked. If this system is one you have added to your arsenal, you will be able to do more than just address the aforementioned concerns. You will be able to show them exactly the kinds of dangers present in the world, and how your system will have no problem maintaining the security of their information.

The defining factors differentiating this product from others is it is a multilayered system which implements biometrics, in addition to other security measures such as digital signature matching, which is constantly monitored, and updates itself each month. By implementing the product, if there are things necessary changes, such as removing a fired or retired employee from the system, security is not compromised. The best part is the potential amount of funding saved as a result of your company not purchasing numerous security systems. It's a package deal and it keeps customers safe and happy, and keeps the company from having its image tainted.

This biometric system would be composed of multiple biometric security checks working together to increase an entity, or system's, security defenses. Some of the biometrics include, but may not be limited to, digital signature authentication and typing rhythm. Biometrics are the kind of security creating a huge barrier against someone attacking remotely, and even internally. This product is a transformation of the basic security system used by most companies because it introduces a new form of security combining different ideas into one unique defense mechanism. In time, the hope is to introduce additional security aspects to the system because one can never be too secure. If you want to ensure your company can deliver when they ensure customer safety, then this system is something you should adopt. The sooner you have it in your infrastructure, the better. If you want more details, we could set up a meeting about additional logistics, and more reasons why this product would serve as a major benefit to you and your company.

Commercial Opportunity

Think back to the event of the OPM breach, and how millions of members of society had their personal information compromised. Cyber security as a major topic of concern until events such as the breach, as well as the influx of cyber attacks recently targeted at health entities, occur. Imagine how much information about and belonging to us is on the internet, in the systems of our places of employment, and in our educational institutions. Numerous entities are entrusted with protecting our information on a daily basis, but just how safe are they? The multilayered biometric security system, Covert Ops, will address the problem and help bridge the gap between a more secure cyber world and the entities maintaining our information.

Despite there being a rise in the attention given to cyber security, there are still not as many industries investing into it. The market is, in a sense, pretty scarce in terms of how many companies are making significant impacts in the cyber realm and/or are investing the necessary funding into the field. Covert Ops is a huge necessity.

There is no specific addressable market for Covert Ops as it is needed in all fields, such as health, education, etc. Every field in some way needs security of information belonging to its customers, or the company itself. If they can't keep it secure, or are not placing as much effort into their security, then they lose their integrity, and the trust of others. Every market needs to invest in some way in their security hygiene. The market of cyber security needs more innovative and reliable methods to combat the individuals with malicious intent. Covert Ops would not only be cost efficient, but save millions of dollars in possible damage from a successful cyber attack.

In regards to the business economics, as mentioned earlier, a significant amount of money is used to drive and address the field. Companies are making themselves more likely to be breached by paying for rudimentary security policies and standards just to meet company standards. Security costs money and to put it to figures, investing over a million dollars into it has become the standard. The money goes to research, development of products, monitoring of systems, and addressing cyber risks, such as malware, botnets, and DDoS attacks. A company's goal should be to do whatever it takes to keep customer information safe and secure.

The validation of Covert Ops on the market is the successfulness of its infrastructure used today. The combination of different methods of encryption and protecting information has historically been perceived as a challenge against hacking. For example, the Vigenère cipher incorporates the Caesar cipher, as well as certain aspects of AES encryption to create more robust protection. In addition, biometrics has been proven to be an extremely effective method of protecting information as it is used in agencies such as the FBI and CIA. Therefore, by investing in Covert Ops, any company would be providing their customers with an additional assurance of their information being protected.

Many products and services, such as Deloitte's Secure.Vigilant.Resilient initiative, have been successful in addressing security vulnerabilities before they happen, after they become a serious problem, and constantly monitoring systems to ensure nothing suspicious is occurring. However, even though the available services seem to address the problem in different

capacities and at different stages, they are still, for the most part, one-sided. Covert Ops takes it a step further by ensuring certain incidents should not occur. Not only would it help alleviate some of the risks arising from overlooked possibilities for one to get into a system, it would greatly improve the market by setting the standards for current products.

The customers for Covert Ops would be any company with information they want to keep safe and its business model will ensure it is extremely difficult for information to be leaked. The creation of the product would be handled by the software engineers and security professionals. There would be a chain of command in place to ensure the product isn't handled incorrectly, and help guarantee everyone isn't able to tamper with it. The funding for the product would come from the revenue my company accumulates, external stakeholders, and any business investments the company has made. Revenue would come from the sales of each product and external stakeholders who would help fund operations in the company.

The competition in the cyber security market is pretty strong due to many companies having a well-established name and tenure. All of their products follow the model of providing customers with protection against unauthorized access, monitoring of their systems to ensure they aren't getting attacked, and recovery services in the case they are successfully breached. I expect the landscape of competition will change a great deal by the time Covert Ops enters the market as more companies are beginning to invest in cyber security. Pretty soon, most of them will have some kind of product on the market aimed at addressing security risks and concerns. The increased interest in the cyber security market will make it harder for companies to get their product to sell, and for customers to make a choice of which product to purchase.

One of the key risks to bringing Covert Ops to the market is it has not been implemented in a company since it is a brand new product. The reasoning behind the risks is a customer may be less likely to trust a product not implemented in companies, and proven successful. In addition, if they have a product they are using now, they may want to avoid the risk of trying something new with the potential to fail, and cause long-term damage. The two aforementioned risks contributes to a third risk - the product does not work properly and does more harm than good to a customer. The risks will be difficult to address in the beginning, but not impossible to overcome. It would take strong efforts in gaining the trust of a customer and convincing them of the potential Covert Ops has to guide them in the right direction.

Most of the finances needed will be for the development and management of the product, consistent updates to ensure it is able to address security risks as they arise, and avoidance of possible intrusions on the product itself. Assuming Covert Ops is able to sell on the market to numerous customers, and my company is able to build strong, long-lasting relationships with different entities, revenue projections could start from 30-50 thousand dollars, and increase to the 10-30 million dollar range. It has the potential to grow and be given additional features to make it more attractive to customers. As mentioned earlier, the economic impact would be astounding as it would help save millions of dollars. The millions saved may have ended up being used for damage control in the case a company is breached. The savings would allow the company to use their funding in other areas of need. In fact, it could help improve the company's standing in the market compared to its competitors, as they would be seen as more secure and reliable. However, one can not put a price on the trust and integrity Covert Ops would help preserve.

Broader Impact

If Covert Ops were used widely, it could help address the concerns many companies have regarding the safety of their business. The answer would be yes, and in turn, Covert Ops would help society as a whole because the information people have entrusted to different companies will be safe. They can have peace of mind knowing their information is in good hands, and they won't fall victim to another scare such as the OPM breach. There aren't specific groups Covert Ops would impact because it would affect everyone. We all have our personal information in the hands of some entity for different reasons, such as our taxes we submit to our schools, and we would not want our information to be handled or given to just anyone. People want to feel safe. We all have enough stress to deal with on a daily basis, and adding your information being in the hands of someone with malicious intent would not improve our lives in the least bit.

There are no environmental or health issues associated with Covert Ops. It is still being determined if the product will be a program or a physical product. Regardless of the fact, it would be child-friendly and simple to use. It will need constant regulation to ensure it is running properly and up-to-date on any new security risks. The management of the system would be handled by the security and technology team responsible for its development and surveillance. It does have the potential to be used for the wrong purposes if the system itself was hacked and used to keep authorized users, as well as the company itself, out of the company's system and database. The chances of a hack on Covert Ops are extremely low as the product will be managed on a consistent basis to ensure it passes security checks, and is as secure as possible.

Covert Ops does have the potential to have a global impact if it is bought, used, and/or has its methodologies used by foreign entities. The product is not necessarily country-specific, as it serves the same purpose in whatever system infrastructure it is apart of. Therefore, it is also not limited to solving problems only in the US. It could help improve security overall as it would provide safety assurance for customers wherever they are in the world. Cyber security could be enhanced and improved on a global scale as the number of breaches would reduce, and the chances of people having their personal information compromised would decrease significantly.

The main global issue related to this product is the growing need for more secure systems and companies. Personal information is held by numerous entities who have the task of keeping it safe. Hackers become more creative by the day with their methodology of attack, and their must be security measures in place to combat them. Covert Ops will be a step in the right direction as it brings it's infrastructure into the field to change the way cyber security is thought of, as well as reduce the amount of successful attacks in the future.

Covert Ops could potentially be used for unethical purposes. One example could be a case of certain people managing the system deciding to keep other individuals within the company out for personal reasoning, or gain. In addition, if the company decided the product should be charged for a higher rate than necessary, or hindering certain features from being used in an attempt to receive more payment from customers, their act would be unethical as well. The product should only be used for the purpose it was made for, and not manipulated for the gain of certain individuals, or for the exploitation of its users. To combat the potential

danger, employees would be required to go through ethical training, among others, to ensure they understand how the product who is to be handled, which individuals manage the system, how to report if there is a belief the system is being misused, and ensuring the company practices are legitimate. The trainings would help to make people less likely to use the system incorrectly, and show customers their information is safe from both internal and external attacks.

Technical Discussion and R&D Plan

Covert Ops is a multilayered, biometric product composed of digital signatures and a typing rhythm authentication system combined to create an extremely powerful security system for whatever it protects. However, it comes with potential technical challenges. For this reason, it is crucial to understand all of the problems and where they stem from.

The first technical challenge is the devices used to create the product. One of the devices used was a Kinect 2 sensor and it handles the digital signature of the product. It is operated through Java code with the ability to allow a user in front of the camera to draw their signature in the air while the Kinect detects the motions of the x, y and z Skeleton coordinates of a person's hand, and then it is compared with the signatures in the database to check if the user is authorized to have access. This idea presents a technical challenge because if Covert Ops is implemented in a company's infrastructure, and another device is used besides the Kinect, then the code has to be changed and implemented differently. In addition, the methodology would shift as well since the methods of drawing and displaying the signature, saving it to a database, and how it is compared would need to work with whatever system implementing it.

The second technical challenge would be the process of confirming one's typing rhythm. Typing rhythms are currently documented through training and tests run to differentiate one user from the next. If Covert Ops were implemented in a company, depending on its infrastructure, certain pieces of the code may not work, and the amount of training necessary will fluctuate depending on the authorized users. This transition could be done during the onboarding of new employees, but would take a great deal of time, and trial-and-error, to ensure the system is configured properly for each user. If there is a small variation or degree of allowance for the typing rhythm, a company runs the risk of possibly creating a backdoor for a bot or an unauthorized user to gain access.

The third technical challenge is the integration of the product into the company's current system. The challenge stems from being able to combine or override current security utilized in the company's mainframe. Covert Ops could run concurrently with the current system, but it may lead to more potential security holes possibly being exploited. The best option may be to remove the current security system and have Covert Ops replace it, but the same challenge of integration still stands, as it must work seamlessly with the company's current system to ensure business can run as normal. This would possibly require the system to be turned down to have the changes implemented, as many things within a company require authorized access. Therefore, business would need to stop to ensure Covert Ops is installed properly and configured to work with the company's mainframe of operations.

The risks with bringing Covert Ops into the market is it potentially becoming a target for individuals with malicious intent to hack into, is a new product with a lack of experience of being tested with actual companies, and it potentially not working as well as current products on the

market. Since this product is new, it has not been tested as much as current products have. The products on the market have most likely been attacked or had hackers try to compromise their system. As a result, the systems have gotten stronger and more prepared for potential intrusions. On the other hand, you have Covert Ops entering the market as a new product without the crucial experience and exposure. The inexperience may cause it to become susceptible to attacks, which would put the company in danger. If it was used in a company and worked, it also may not be as good as other products out, which makes the reasoning for using it less relevant as a company could use the product it already has installed.

In the Phase 1 project, I will focus specifically on the third technical challenge - ensuring Covert Ops can be integrated properly into the system without mishaps. If Covert Ops works without flaw but can not work with the company' system, then it defeats its purpose. Granted, the other challenges are also important, but can be addressed once the system is in place. With Covert Ops installed, all potential complications are addressed realistically and solutions are substantial. In addition, the solution to this challenge will help address the other possible issues because the core of the problems stated is ensuring the product works properly for the company. In a sense, solving this challenge is essential to handling the rest.

The innovation behind Covert Ops is an orthodox as it is simple, yet complex. It is two-fold: it implements a method of security not used by many companies today and incorporates unconventional security measures which make it more difficult for individuals with malicious intent to gain access to what they seek. The innovations mentioned are necessary as it introduces new methodology hackers may not be accustomed to, which in turn poses more of a challenge to them. Granted, there are arguments stating it is a more secure option to use security methods already in place as they have been implemented and tested for years in the field. However, even though the methods have been tested against attacks, the one fact still stands of it being impossible to create the perfect system. Therefore, new methods of security must be introduced, or combined with current measures, to continue to ensure security for customers. This reasoning can be seen in the updates offered for different mobile applications encouraging its customers to keep their software up-to-date to ensure new threats arising are dealt with. Cyber security is constantly changing and becoming even more creative. As a result, companies must continue to keep up their countermeasures to keep critical information protected.

Covert Ops implements a method of security not used by many companies today - layering their security measures in order to create a more complex and robust system. Historically, multilayered systems have tended to be more secure as it is not enough to simply crack one password, or pass one line of defense. In Covert Ops, the two lines of defense are the digital signature recognition and typing rhythm authentication. Combining them poses a major challenge to hackers as the two defenses are very personalized to the users. It is extremely difficult to mimic a person's typing rhythm and signature. Even though a person may not type the same speed at all times, or sign a document the same way each time, there is only a certain degree of variance where it is no longer their normal pattern. The digital signature works by capturing a person's signature in real time through hand movements detected by the Kinect sensor, saving it to a database - possibly a SQL database - and comparing it to additional signatures stored in the database. The comparison will either be conducted using the

coordinates of where the signature is painted on the screen or by comparing pixels of the image to others previously saved. There will be a certain level of tolerance in how accurate a drawing on the Kinect must be in order for it to accept the signature. The typing rhythm is a more intricate level of security as it is a training system documenting how fast a person types certain statements, if their speed is constant or varies, and how they handle typing different bodies of text. The user will be asked to complete several prompts, which will train the system to recognize a user and their typing rhythm, which will reduce the need for a high tolerance in the system when it comes to determining if a user and a rhythm match. The benefit of using the biometrics mentioned is they are personalized, and much more difficult to adapt. In addition, they must be done in person, which reduces the risk of outside threats gaining access as well.

The second innovate piece of Covert Ops is its incorporation of security measures posing a challenge to hackers - digital signatures and typing rhythms. Each uses Java programming methods and libraries to both train and differentiate one user from the next. These libraries include the GUI components, J4KSDK, and others. For the digital signature portion, there will be a bounds in the screen serving to limit how large a signature can be, and if a signature falls outside of the bounds, it will throw an error. When the comparison piece is started, the bounds will help reduce the need for a high tolerance of variance in the signatures. The innovation of this portion of the security comes from it being difficult to match the signature of someone else due to the fact every person has a unique writing style. A person's style will affect how the signature is drawn and how close it can be to someone else's. This difficulty makes the system more secure and less likely to by breach. The training portion relates more to the typing rhythm as the system will prompt the user to type certain statements and based on characteristics such as speed and consistency, it will document the results and use them to create an average. This average will be used to mark users, match them with a typing rhythm to be saved to the database, and determine whether or not they are authorized. The benefit this intricate system brings is it creates a sturdy barrier against individuals attempting to gain unauthorized access to information not belonging to them. The biometrics presented have the potential to change how security is thought of and how current methodologies can be improved to be more effective and secure.

The key objectives of the Phase I research will be to determine how compatible Covert Ops is with the system it is implemented on, the speed and diagnosis of the product when it is run, and what other requirements the product needs in order to run properly. During Phase I, the overall goal is to get a better sense of how Covert Ops would work in conjunction with another system. The compatibility would be determined by attaining the system information of an entity such as the programs being run, the operating systems it executes on, and how the infrastructure itself works. With the system information, it can be determined if Covert Ops is compatible enough to run seamlessly when incorporated. Actual tests would need to be run to formulate a diagnosis and document the speed at which the system runs with the product in place. The results will be very useful in helping to get a sense of what additions Covert Ops would need to work for the company without errors. If the tests are not yet run, then a report of the current system will need to be obtained from the company's security and IT team. Then, estimates can be made and the necessary actions can be acted on for the product.

Along with the objectives being accomplished during the Phase I research, there are also questions associated with them in need of answers to ensure Covert Ops can be properly integrated into the company's security system. The questions in need of answers are as follows: can Covert Ops be integrated into the system without interrupting the current system; does the system run as normal with Covert Ops in place, or is there a change in speed; is it feasible to have the system shutdown to install Covert Ops without affecting business; what systems can Covert Ops be incorporated into; what other capabilities or technical additions does Covert Ops need to work with the system; will the cost of the product depend on the amount of places it is needed or will it be one set amount; how much funding will be needed to maintain the system, bearing in mind the cost of technologies and implementing it into the company system; and what processes must be followed to fully integrate Covert Ops into the current system, and replace or add to security measures already being used? To get the necessary answers, in addition to the discussions with the security and IT team, data will need to be obtained about the current security system and a diagnosis of its results since being implemented with metrics around security hygiene, and the amount of funding needed to keep the security running.

The critical technical milestones necessary for Covert Ops to market are being adaptable enough to be integrated into whichever systems using it, a fully functioning real-time reporting system in the case an error has occurred or a threat is detected, daily diagnosis reports, and lifelong assurance. Adaptability is crucial as the product must be able to run properly on any system it is implemented on or it becomes useless. A detection system can be added to Covert Ops to learn the system information once it is installed and make the necessary modifications to work in conjunction with it. The reporting system is necessary because if a problem arises in which the company using Covert Ops must be aware of, or has reported, it needs to be addressed immediately to avoid the system being compromised. The report will be generated by documenting the time it takes for the system to detect a problem and relay it to Covert Ops headquarters. Daily diagnosis reports will be useful in this case as well. They will note if the product is improving the system, running properly, and addressing concerns as they arise. In addition, it will show the company what areas they may find problems and what kinds of threats they should be cautious of. The last milestone - one of the most important technical milestones - is lifelong assurance. Companies need a product with the potential to last, and if Covert Ops has limitations in how long it can provide service, it will not last in the market. Companies need assurance of their product being able to overcome any challenges for a long period of time. By continuously updating the product and conducting a diagnosis on it, Covert Ops will be kept in working order, running effectively and efficiently.

The objectives of the R&D plan will be to attempt and successfully integrate Covert Ops into a company's system, test its performance, document any errors and/or complications, and review the diagnosis in order to determine the necessary changes to be made. In the first month, Covert Ops will be brought to the company and installed into the system. Different installation methods will be conducted to determine what system requirements are needed for Covert Ops to be incorporated and run properly. The result of the R&D plan will be a refined and efficient product ready to advance current security measures and protect customers for years to come.

I. Initialization of the Kinect and its libraries - **Complete**

   A. Install the Kinect libraries
II. Run the Demos - **Complete**
   A. Have all demos running correctly and fully functioning without problems
   B. Determine which demos to use as a foundation for Covert Ops
III. Utilize Skeleton Class to Set Bounds - **12/15/2016**
   A. Create signature bounds on the screen for the user to draw in
   B. Set a time frame to draw signature
IV. Implement Kinect Paint Libraries - **12/15/2016**
   A. Find and utilize Kinect library to allow users to write on the screen
   B. Import all necessary libraries
   C. Begin finding ways to integrate into current project
V. Test Bounds and Paint in Conjunction - **12/31/2016**
   A. Combine the code of the paint and the bounds to work together
   B. Debug the program
VI. Capture Digital Signature and Compare - **01/30/2017**
   A. Implement an algorithm that will either compare images or signature coordinates on the screen to match user to signature
   B. Test with numerous individuals to differentiate
VII. Begin Combination with Typing Rhythm - **02/28/2017**
   A. Start integration of the typing rhythm authentication with the digital signature program
VIII. Create Interface of Covert Ops - **03/15/2017**
   A. Use Java GUIs and other libraries to create an interactive interface for Covert Ops
IX. Testing System and Completion - **03/31/2017**
   A. Test Covert Ops with multiple users to differentiate users and determine authorization purposes
   B. Debug system and database holding information