Patriot One

October 2016 Pilot

|	
Version:	**1.0**
Submission Date:	**2016-05-25**

Authors: Meaghan Reinecke
Faraz Rahnemay

1 Background and Context

Macadamian is collaborating with Patriot One Technologies to bring a threat detection technology to the market. This disruptive solution can detect weapons in noncompliant subjects, using signal processing to match radar detection against a neural-net-powered database of unique weapons signatures. This solution will be a low-cost threat detection for concealed weapons, where no security solution currently exists.

Our pilot project will install the solution at two different test facilities, and we will 'road-test' the technology with real participants and real security teams. These pilot locations will be critical in assessing the viability and scalability of this security technology. The data collected in the pilots will help improve the design, as Patriot One prepares for the April 2017 alpha launch.

We work in an iterative, high-touch fashion -- our next steps together will be the high-level design (including paper prototyping) of the entire customer experience, as well as software architecture and back-end services. This first phases -- done in parallel with aligning equipment vendors and hardware providers -- will support a tighter range and more detailed project plan for the entire development piece. To that end, we have included ranges for the investment of the entire software development, but those ranges, milestones, and project plans will become more firm as we complete our first phase of 'HIgh-Level Design and Architecture'.
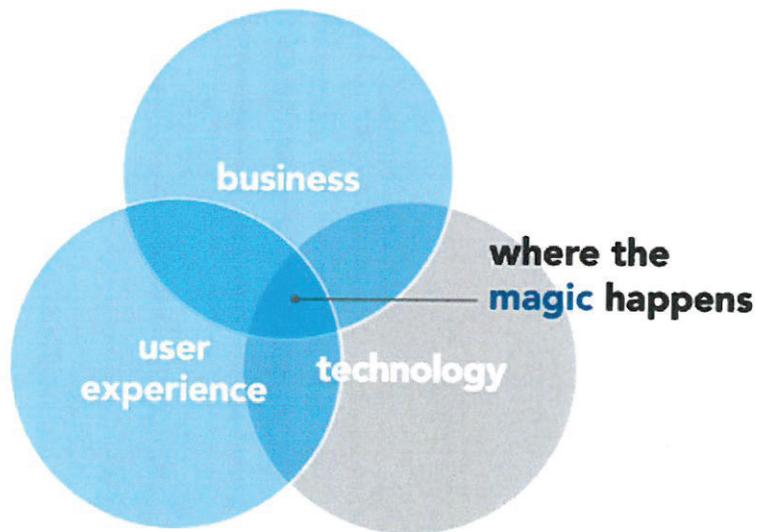
GREAT DESIGN involves an understanding of the business and the users, as well as the technology possibilities and constraints

2 High-Level Approach

2.1 Structure of our Approach

We propose to kick off this project like no other partner. We propose to approach this project in four phases:

1) Discovery

    The discovery phase will be both: a) intensive high-level design, and research at the proposed pilot locations, and b) alignment with hardware design.

2) Design and Development

    UX design, software development and test teams will be collaborating to create the software design and development to support the requirements of the pilot locations at an acceptable level of quality to be ready for deployment.

3) Deployment and Knowledge Transfer

    Efforts will be required to support the set-up and deployment of the Patriot system at the two proposed pilot locations. There will also be some time required to ensure the Patriot team is prepared when monitoring the system as it's running.

4) Support and Maintenance

    We anticipate that Macadamian will provide support and maintenance during the pilot phase. However, the efforts for this phase will be covered by a separate contract, to be developed as the pilot launch approaches.

Our approach looks at the scope as a funnel -- we can provide a lot of details about the immediate next steps, in terms of effort and investment estimates and detailed accounts of deliverables. The further along the timeline, the details are less-defined and the estimates of effort and investment have a wider range of possibilities. To that end, this proposal provides a significant amount of detail for the Discovery phase, some ballpark estimates for design and development, and ideas and recommendations around support and maintenance. At multiple stages throughout the project, we will provide updated estimates around efforts and investment, and weekly updates on timelines and progress.

We feel it's important to highlight the relationship between the Discovery and Design&Development phases: we may learn about key or critical information that has an effect on the plans described here. This proposal represents our hypotheses and prediction about our approach, as a result of collaborations with multiple experts. Upon testing our hypotheses, we may recommend changes to this plan. We will always communicate with you fully, and provide all information we can, when seeking your approvals and inputs into decision points.

High-Level Plan for Discovery. The following table illustrates a high-level plan for the discovery phase of the engagement. Both phases will be done in parallel.

High-Level Design & Research	Architecture & Hardware
Macadamian Design and Research go onsite to the pilot locations -- here, they conduct requirements gathering and observation with security. They create some early design ideas for quick validation with end-users. Deliverables are: • Physical requirements, based on environment and security system	The lead architect and project manager will go on site to Sensoft to work with the hardware design team. Deliverables are: • Updated High-Level System Design & Architecture • Concept design of all technologies for working architecture • Integration Plan • Deployment Plan

• Design requirements, based on existing system • User requirements, based on end-user interviews and validation of design concepts	• Identification of required 3rd-party services • Project Plan for *'Design and Development'* and *'Deployment and Knowledge Transfer'* Phases
Outcome: Support understanding of unique requirements for pilot locations, user validation of initial designs, and prioritization for remainder of development project and design	**Outcome**: Provide solid, feasible software architecture implementation, based on best practices and proposed infrastructure & constraints
2-3 weeks	**2-3 weeks**

High-Level Plan for Design and Development. The Discovery team (IxD, Rx, Arch and PM) will reconnect to define and confirm the full scope definition for the MVP development. Updates and changes to these initial estimates will be done at the end of Discovery, leading into this 'design and development' phase. This may include high-level estimates for the Deployment and Knowledge Transfer for both pilot locations.

For details about our integrated approach in 'Implementation', see section 4.2.

Projections for Support and maintenance. For the pilot phase, we anticipate that Macadamian would provide admin and support services, on behalf of Patriot. The estimates for effort and time will be covered by a second SoW, which will be produced as the pilot dates approach.

2.2 Deliverables for Discovery

The deliverables for this engagement are as follows:
- Design Concepts and Mock-ups
    - proposed low-fidelity designs for screens used by security personnel
- Research report from both customer and security personnel
- Functional integration points of key pieces of architecture
- Finalized concept design for technologies (based upon the architecture design)
- Detailed project plans and timelines for all remaining work

There will also be secondary work products along the way in support of these primary deliverables, such as sketches, meeting notes and so on. Also, the expectation is that the work done in this first phase will provide scaffolding and momentum for the entire project. Because the software team will be dependent on hardware, we currently project a small pause between Discovery phase completion and the ramp-up of the Development team as they wait for hardware to be ready. The Design team can proceed, and is not dependent on hardware.

2.3 Resourcing Timeline
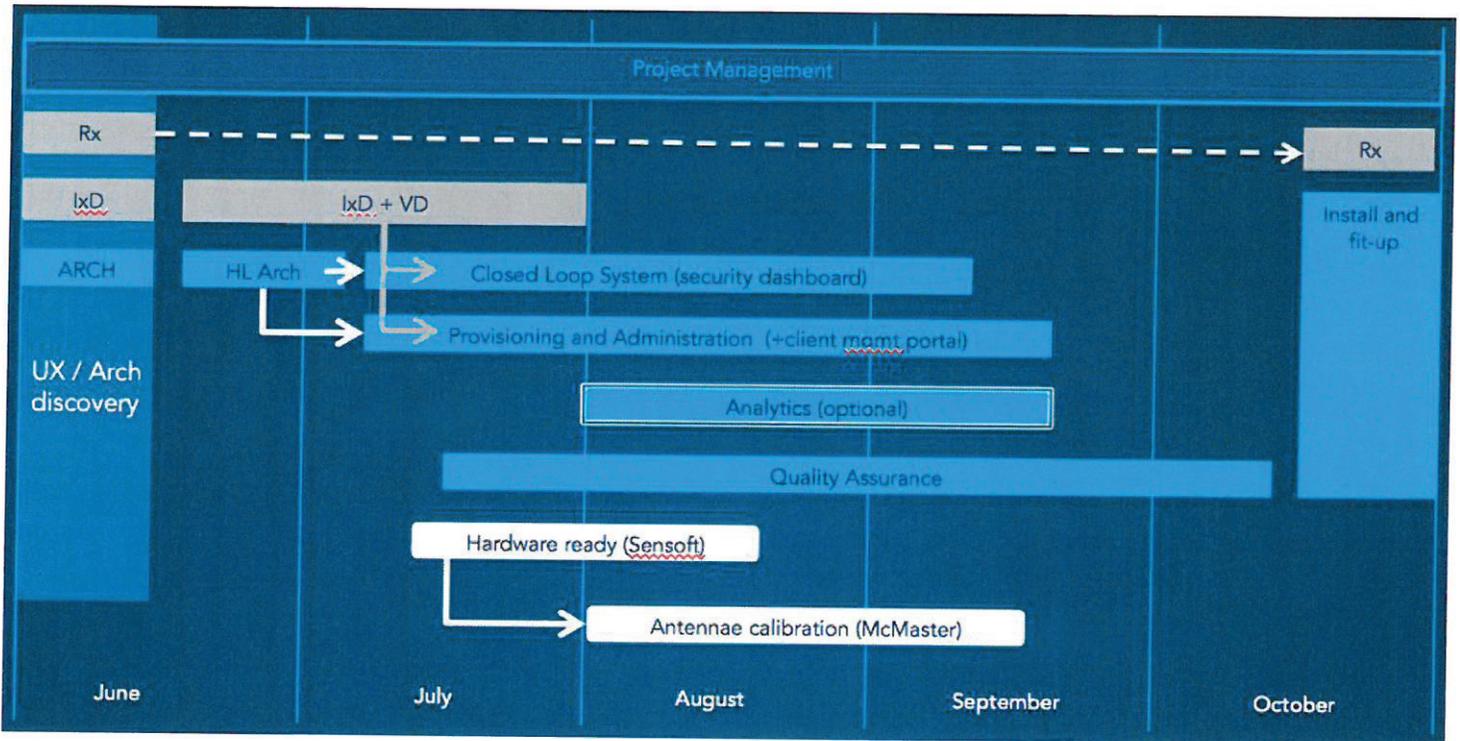
The above diagram illustrates the proposed team composition and schedule, with rough outlines of timelines. Details of specific dates are not defined. Also, **there will be a high degree of overlap between the 'Antennae calibration' team and the larger software teams, and dependencies here may cause delays to this proposed timeline**.

3 Discovery Activities

3.1 UX Discovery

The goal of this engagement is to achieve a successful pilot deployment of the radar technology -- to that end, it is critical that the team understands the details of the pilot locations. The Lead Designer and the Lead Researcher will travel to the pilot locations (currently targeting McMaster University and an arena/stadium). On-site, this team's activities will consist of:

- Interviews with key stakeholders and end-users (i.e., Campus/Stadium Police leaders, the users who will be monitoring the system, and the IT department responsible for installation)
- Observations about the workflow of the campus/stadium police (specifically, watching other monitoring systems and the inputs/outputs of these)
- Recordings of user requirements, specifically key information required for decision making
- Early concept sketches for walkthroughs or early user validation

We expect the UX team to be at each pilot location for about 2 days, and would engage with key stakeholders/users over multiple interactions.

The team will complete this first phase with a solid understanding of specific requirements for each pilot location -- supporting custom installations and deployments for each location.

3.1 Architecture Discovery

The Lead Architect will need a high degree of collaboration and alignment with the hardware team. To support this, the Lead Architect will travel to Sensoft to spend a working week with the hardware team. This group will align on:

- Board design
- On-board (or chip) code
- Provisioning
- Communications protocol
- And any other critical elements where the software and hardware must communicate

The role of application architect is to create the big picture, identify and clearly outline the best technologies and patterns, and understand all other partners' hardware and technology contributions. As the architectural overview gains clarity, the application architect and project manager will collaborate on project planning, drafting of technical documents and high level architecture to aid in the rapid ramp up of the development team. Prototyping may be used in key areas to de-risk gap areas and demonstrate design concepts.

Key responsibilities include:

- Identify key high-level components, platforms, and services required to deliver the solution
- evaluate 3rd-party services vs. custom implementation
- make recommendations for using 3rd-party service providers or custom implementation
- provide outlook and impact of recommendations with respect to CAPEX and OPEX
- create the high-level software architecture
- plan out cloud infrastructure and deployment strategy
- map out requirements and solidify scope for post pilot phase

3.4 Project Management

Our project managers are experienced in managing the multiple dependencies between design, research, and architecture, and provide the key administrative support (about timing, budget, scope, etc) in order to allow the delivery teams to focus on their respective crafts. For this project, the project manager is expected to be involved between 1-2 hours per week for the first 4 weeks, and then more heavily involved in the final two weeks as they collaborate with the architect to create the detailed development schedule and task breakdowns for the entire development process.

For this engagement, the project manager will also interact with Sensoft to understand key timelines and dependencies, as well as clearly outline responsibilities and scope for Macadamian, as it relates to work being done by the other two collaborators.

3.5 Transition to design and development

Both the UX team and the Lead Architect will collaborate on the prioritization of design and development activities for the remainder of the project, leveraging the Project Manager for sprint planning and coordinating team ramp-up. We expect a seamless transition from Discovery to Design and Development.

The development team will be dependent on the hardware availability -- this may result in a 'pause' in the cadence of the

project. We will optimize the schedule to ramp-up the development team on an as-needed basis. The architect will spend efforts towards the high-level architecture, and standing-up any elements that can be simulated.

4 Design and Development Activities

4.1 Interaction Design

The information architecture, key workflows and associated wireframes will be evolved from the concept sketches done in Discovery. This will be a highly iterative process that involves internal stakeholder feedback. The design team will also work alongside Sensoft to respect the hardware requirements and form factor to support infield troubleshooting and ease of deployment.
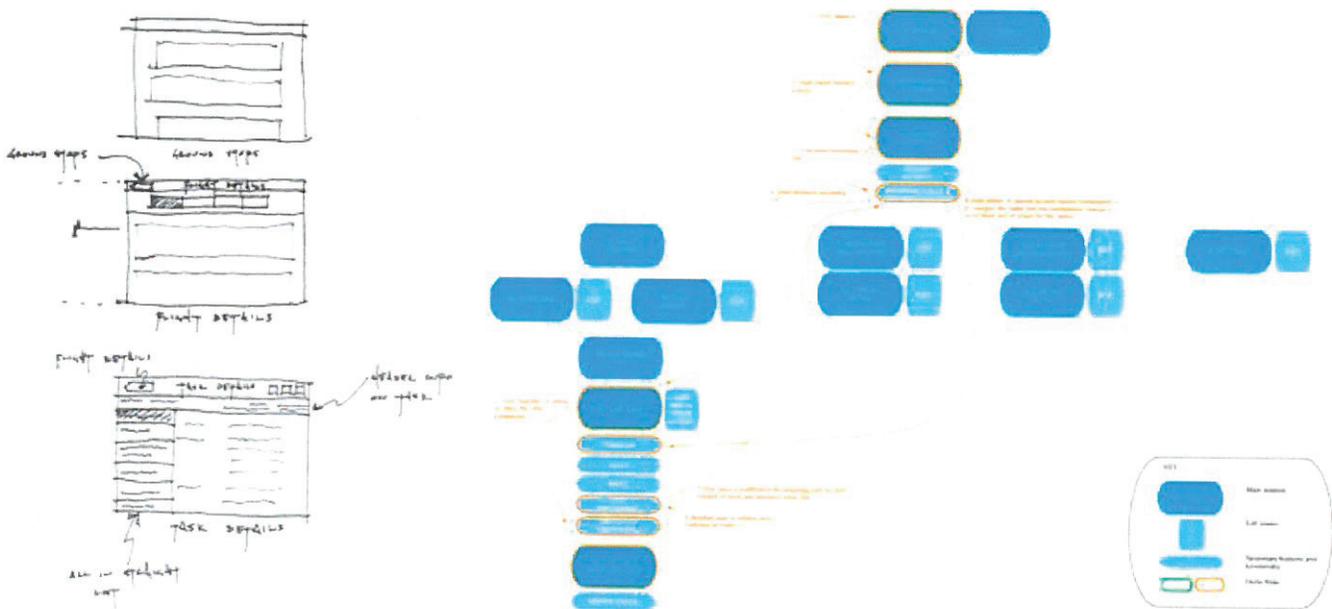
Examples of early design concepts (left) and Information Architecture with workflows (right)

The design team will iterate their proposed interaction designs according to stakeholder feedback (including software and hardware teams). The final design deliverable will be annotated wireframes, describing interactions and screen behaviour that can be used by the development teams. The majority of the interaction design and wireframes will be spent on the tenant system (that faces the security guards), and any remaining effort can be directed to support the admin system.
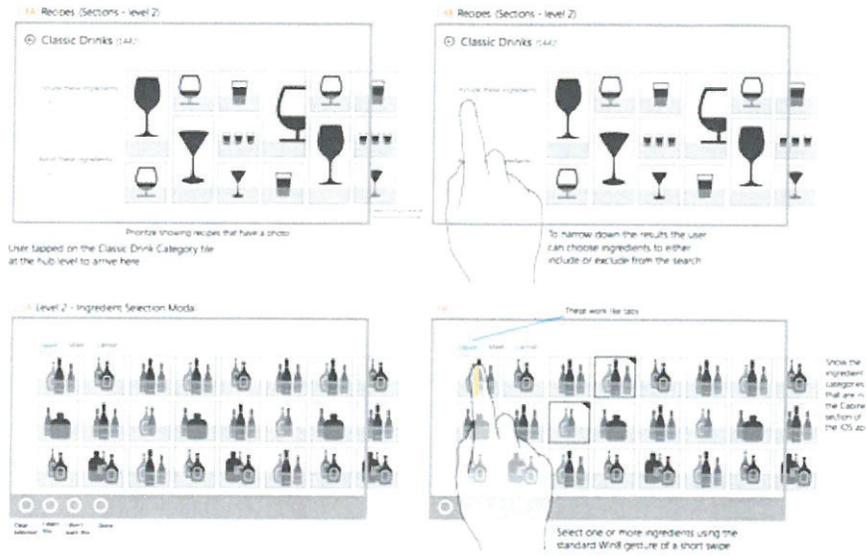
A more detailed wireframe with annotations, required for development

4.2 Visual Design

Macadamian will create two major options of the look and feel for the areas of the application that face the security guard (currently referred to as 'security dashboard'). These will be based on two different unique wireframes. This will allow the product team to get a better sense of the overall look and feel without having to do a visual comp for every wireframe. These will be high fidelity comps reflective of the actual final production quality visual of the software (see sample below). Macadamian will use the Patriot branding and style guide to drive the overall look and feel of the final visual polish.
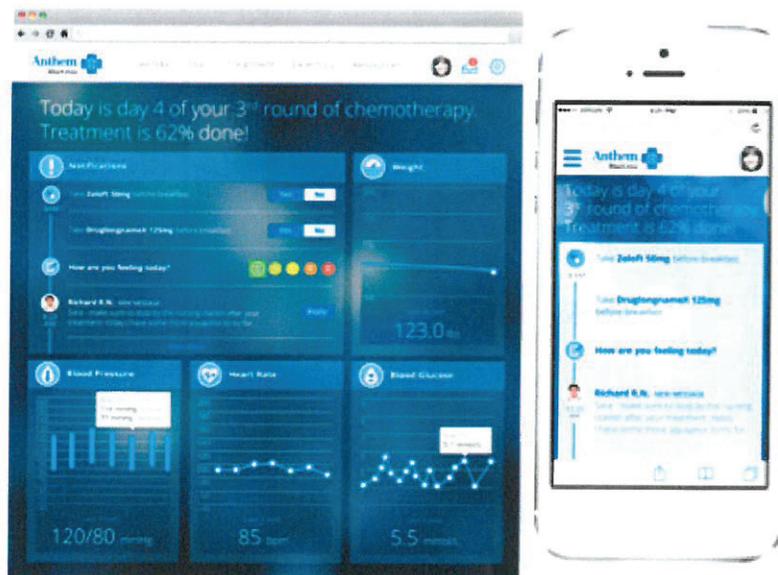

Samples for our design portfolio, supporting two form factors

Visual design can be subject to a high degree of churn. To manage that, the lead visual designer and the Patriot project team will establish a cadence and desired number of design reviews. The number of design reviews translates into more days of work, so it is prudent to decide the number of iterations in a kick off meeting. This will be left to the discretion of the visual designer and the Patriot project team.

4.3 UX Design, Development and Quality Assurance

Our approach is both collaborative and cross-discipline. We work seamlessly as or among agile development teams on a daily basis. In fact, Macadamian has developed a highly effective model for integrating UX into the Agile product development process (as shown below).
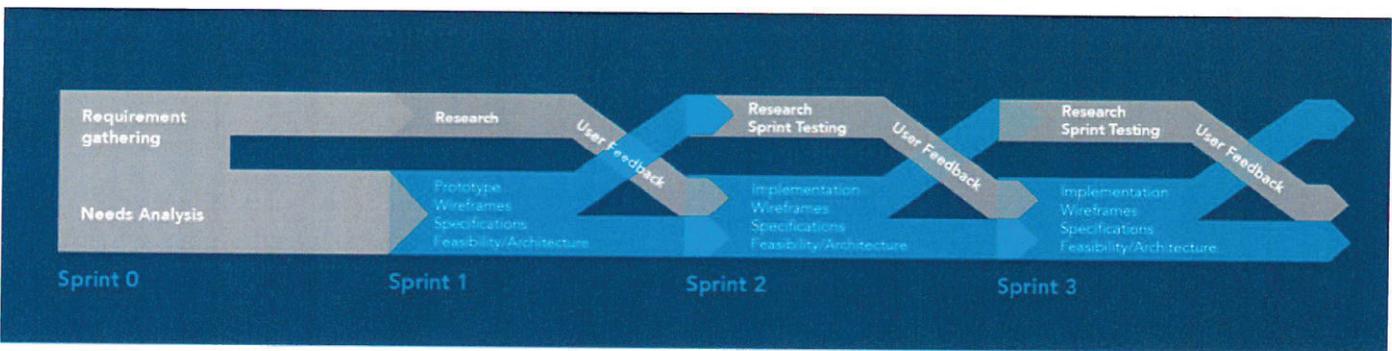
The essence of integrated process is simple – an initial sprint zero to define the UX roadmap, while the development team plans the architecture. After that, the UX and development teams work in 2 or 3 week agile sprints following a scrum process, with the design team working 1 sprint ahead of the development team. The key is not the process itself but the daily communication throughout the project, and the thorough understanding and appreciation that team members need to have of each others' roles and how they work together. Our developers know how UX research and interaction design work, removing friction that is often seen when UX and development teams try and work together. Similarly our UX team members thorough appreciation for software development, removes the risk of getting a "blue sky" design that looks great on paper but can't be reasonably implemented.

Moreover, we engage with cross-functional client teams, including: strategic and technical product management, software development, design, business analyst and marketing groups. Our team welcomes the opportunity to create the results you are seeking with this important project.

4.4 Considerations for leveraging existing IP

Macadamian already posses existing IP and can subsidize additional portions of the project in exchange for retaining IP rights for generic modules and infrastructure. The estimated build-time of the lab IP amounts to approximately 2 months of development effort, and is available for use for a one time fee of $20,000 for granting a non-exclusive license to be used only for this product.

4.5 Considerations for installation and deployment

Decisions made regarding provisioning will have a direct impact on the installation and deployment at the pilot locations. Additionally, critical information and learning here will help improve installation for the alpha product, later in 2017.

5 High-Level System Architecture Considerations

5.1 Prioritization of Architecture and Functionality

The system can be broken into two major sets of components; "critical", and "value add". The critical functionality refers to any feature or component allowing the device to detect dangerous objects and to trigger alarms on the security dashboard. Without this workflow working properly, predictably, and reliably, the system as a whole is meaningless. The "value add" areas should be considered to enhance the experience, and should only be included in scope if both time and budget permit.

1. The first component of critical functionality is the **closed loop system**. Running the system on a secured closed-loop (and therefore, on premise) solution is the most important element to have in place, and provides a working system without incurring any potential risks of cloud or distributed systems.

2. In order to deploy the critical components, and tie them into a functional system, **provisioning** the devices becomes a necessity, and therefore also a high priority.

Beyond these two major elements, the priority to provide system-wide analytics, or other functionality becomes secondary, or "value-add". While a fully functional multi-tenant system may well be desirable in the long-run, we expect to prioritize resources toward ensuring that all the critical components of the closed loop warning system are fully functional and provisionable prior to putting resources into the value added services. This will help de-risk the deliverable by ensuring that the greatest business value is delivered first and therefore less at risk if any unforeseen slips occur in the project execution.

As each of the other system considerations are discussed in the sections below, the architectural decision to should consider first; whether it de-risks and assures the critical functionality for the pilot phase, and second; whether for similar or reasonable amount of additional effort, grants far greater system extensibility.

5.2 Multi-Tenant, Single-Tenant and On-premise Deployments

Given the parameters discussed during the workshop, one of the considerations for the system centers around the ownership and stewardship of infrastructure. This determines whether we produce a stand-alone deployment model isolated for each client (as a single tenant system, or an on-premise deployment if it's hosted on the client's own servers), or whether we create, own, and maintain a singular infrastructure platform for all clients to use. In preliminary discussions, we are projecting that we will deploy single closed-loop systems for each pilot location, keeping in mind that a market-ready product will likely need to take advantage of a cloud infrastructure. There will need to be judicious trade-offs between what is low-risk for the pilot project, and what can be re-used or maintained for the larger product roll-out.

Patriot One will eventually want to deploy its own cloud infrastructure, and all clients will subscribe to it for usage. This will make

maintaining, deploying, and enhancing existing and new deployments easier to manage, at the risk of having a single point of failure for all clients. This risk can be mitigated to reasonable degree as discussed in the later section under *security and reliability*.

The desire to have all clients using a cloud deployed service however, will need to be counterbalanced by the other operational assumption, which is that the alarm functionality of the devices (events and alerts regarding the detection of prohibited objects) will be communicated on a "closed circuit" using existing network infrastructure. The point here is to minimize reliance on any portion of the network that isn't absolutely essential to complete the message loop between the device and the security console. This will reduce tampering, hacking, and swatting risks as well as decreasing latency. Furthermore, the shorter and less complicated the path for mission critical communication, the less likely it is to suffer network failures.

Therefore, whether the cloud component is single or multi-tent, on-prem only or cloud-base is an architectural choice the justification for which will surface during the discovery phase. However, that choice should not violate the requirement to keep critical communication closed, and secured.

5.3 Network Infrastructure Security

During the workshop, we heard our security experts express concerns around the perception of cloud infrastructures as being inherently unsecured. However, we need to counter-balance this problem of perception against the complexity of not using existing and proven infrastructure platforms such as Azure, AWS, and the like.

The reality of the matter is that security is no more guaranteed with a "privately" hosted platform. Security is a system-wide consideration that must be accounted for at all levels of the solution, including the server platforms that host the services, whether "public" or "private". The advantages of using one of the primary cloud platform providers includes scalability, standardization, and therefore relative commoditization of expertise required to stand-up, deploy, and maintain the solution over time. Put plainly; cloud gives us an elastic platform that scales to growing demand, provides backup and redundancy features as necessary, can be secured like any privately hosted service, and due to its prevalence in other technology solutions there is a large market of experts with experience so that ongoing work won't cost a premium for niche skillsets.

However, all network infrastructures carry some element of risk of down-time due to system-wide or single-point failures. To mitigate the impact of such events, we recommend that critical events (such as alarms) be communicated directly to a security console via a secured channel on the existing network without any gating reliance on intermediary cloud services. The idea here is to use the cloud services to provide high-level value add functionality, but have a direct, and secure communication line to the security console that could work without external internet access.

5.4 Provisioning

One aspect that needs consideration and further collaboration between Macadamian and SenSoft is the flow and sequence of how devices to provisioned onto the Patriot One system at large, and further tied to a client's account. This process needs to be informed to some extent by UX, and will also be limited by technical constraints regarding how the device is connected to a network, whether it will need to traverse firewalls, and how unique identification will be assigned.

5.5 Security and Reliability

Since this offering is positioned as a security solution, connection and data security, privacy, and reliability will be major concerns for clients. These points will need to be addressed at all levels of the solution. Options to consider include:

- Tamper-proofing and tamper-detection
- Heartbeat for online/offline status to notify if a device has been taken offline
- Securing lines of communication
  - HTTPS and SSL
  - Hardened Administrator Device(s)
    - Trusted Certificates on specific Admin devices
    - Only Whitelisted & Trusted Administrator Hot-spots allowed access to admin systems
    - Use of secured 3rd-party OS images (similar to those provided by https://catalyze.io/)
  - End-to-end audits on all administrative actions
  - Write once, append only logging
- Encrypting data at rest
- Using proven authentication and access control patterns to issue and revoke access to clients
- Redundant and backup services and databases
- Scalable infrastructure deployment built into architecture roadmap to allow spinning up additional resources when load balancing is required
- Developing APIs that inherently support load-balancing (ex. Using idempotent API implementation)
- Building reliable notification delivery into the architecture
- Hardening the on-device OS
  - Using a stripped-down OS to minimize exposure to attack vectors
  - Strict password policies / Hardware Tokens / Multi-factor authentication for provisioning access
  - Strict firewall and network settings

5.6 Notifications

Aside from the fact that notifications need to be generated, the *reliability* of delivery also needs to be addressed. Network failures can occur at any point along the communication path between the device and the security console being monitored for device status and activity. The architecture and workflows need to account for network downtime, dropped notifications, unacknowledged notifications, and retries.

5.7 Client Management Portal

IF we go with a off-prem architecture; as part of the services Patriot One will offer, clients will require a point of access which allow their clients IT or security team to manage their security personnel's authentication and access to the Security Dashboard. This component will need to allow clients to manage roles and permissions, and may also be an appropriate place to access trend analytics information as it becomes available as a feature (budget and timeline permitting). This client management portal should be secured and provide full-audit trails for any administrative changes made by clients.

An on-prem solution mitigates this to a large degree simply by having the whole system physically and network secured on location. Anyone with access to the security room where the security dashboard resides, has access to the system as well.

5.8 Security Dashboard

Within the closed-loop system, the security personnel who are actively on duty will require a mechanism to inform them of any potential alerts that the Patriot One devices might generate. This Security Dashboard will be the daily interaction point between users and Patriot One. Aside from security, world-class UX and fluid and modern UI will help position the product as a security platform designed to endure for the future.

5.9 Admin Portal

While there will be administrative portals to manage services such as cloud platforms, event hubs, and notification services, Patriot One will also require a console for its own administrators to create profiles for new clients, and manage the entire fleet of devices. Trend analytics, if collected (budget and timeline permitting), could be surfaced as part of this portal. Audit trails for all changes made through this portal would be beneficial for security purposes.

6 Team

The following provides role descriptions for the Discovery team. The Design & Development team will be larger, but will have all of these same people included.

6.1 Lead Interaction Designer

Responsible for leading and shepherding our collaborative design process through to the transition to the development phase. Our Lead Interaction Designer will drive the user experience agenda and be ultimately responsible for all design related contributions. This person will create the wireframes and proposed screen behaviour for the software, and continue during the full development project to provide design support to the development team.

6.2 User Researcher

Our researchers all hold post-graduate degrees in the study of human behaviour as it relates to information processing and human-machine interaction. Our user researchers will lead the user research and will be responsible for producing the associated report as well as presenting that report to Patriot One.

6.3 Lead Architect

The Lead Architect is involved throughout the product creation process. Macadamian has a team of senior development specialists who work together to ensure the team makes the proper high-level technical decisions at all times.

6.4 Project Management

Macadamian will provide a project manager who would oversee the delivery team responsible for this initial engagement and support them in terms of project status, financials, issues and risks. The project manager would also collaborate with the

architect to create the detailed estimates and work breakdown for the full development, as well as liaise with the third parties (hardware providers) to sync timelines and understand dependencies.

7 Assumptions

This proposal assumes:

- A Patriot One project owner will be assigned -- this person will be responsible for overseeing the multiple vendors, and managing dependencies between vendors and deliverables. This person will also be responsible for coordinating with proposed pilot locations and the key stakeholders there.
- Both pilot locations will have existing security systems and securable network infrastructure in place. They will not use the Patriot One technology as part of their critical path of security, but as a location in which we can test the product with live subjects and validate against existing security systems. In other words, it can augment but not replace or be used as the primary security method.
- The McMaster team will execute the antennae calibration independently -- should the team require software support, that would be additional to this proposal.
- The deployment team will require the help of facilities and professional installers -- the Macadamian team will ensure the software works once it's physically in place.
- The scope of the MVP covers known knives and guns -- polymers, powders, and custom weapons are not in scope.
- Pilot locations are responsible for providing the following technical elements onsite:
  - A secure local network for Patriot One devices to communicate without external internet attack vectors
  - Secured servers on the secure network capable of serving up the security dashboard
  - IT support for provisioning our devices onto their network, and hardening network access for deployment
    - This includes but is not restricted to firewall configuration, whitelisting device access, closing unused ports, etc.

8 Cost Estimates

8.1 Services Costs

These are effort and budget estimates for the Discovery Phase.
We have also provided **high level** effort and budget estimates for the Design & Development phases that will be validated and refined after the discovery phase.

Note: These estimates **do not** include effort for the "deployment and knowledge transfer" phase which will be covered under project change order when appropriate.

[Redacted pursuant to s. 12.23 of NI-51-102]

Additional estimates for Deployment and Knowledge Transfer:
We strongly recommend that the initial team (PM, Designer, Researcher, and Architect) travel to each pilot location to be present for deployment or to be present once the system is running. These will provide critical support for the maintenance teams, and will help improve the experience for future versions of the product. While this approach is recommended, it's difficult to predict exactly what this will represent in effort and costs, and it should be considered additional to this contract.

8.2 Terms of Business

1. **Type of engagement** - This is a Time & Material engagement, all prices are in CAD dollars and subject to applicable taxes.

2. **Payment Terms** - Client will be invoiced at the end of each month based on the actual hours incurred and the contracted daily rates. Invoices will be due 30 days after the receipt of a properly rendered invoice. Past due invoices will be subject to arrears interest of 1.5% for every 30 days past due. A 25% deposit of $75,000 is due on the execution of this agreement. This deposit will be deducted from the final invoice of this engagement. Credit card payments are subject to different terms specified outside this agreement

3. **Reimbursable expenses** - Patriot One shall reimburse Macadamian for all project related expenditures including travel, lodging, meals, hardware & software purchases directly related to the performance of the contracted services under this project, providing that the pre-approval from the customer has been received. Reimbursable expenses will be subject to an administrative charge equal to 5% of the expenses incurred, provided that Macadamian has received prior preapproval from the Client for such expenses.

4. **Non-Solicitation** - Both Parties to this engagement agree not to solicit or cause to be solicited any employee of the other Party working under any engagement, for a period of no less than 12 months after conclusion of this Statement of Work.

5. **Termination** - Patriot One reserves the right to terminate this agreement "for convenience" with 30 days advanced written notice to Macadamian. Upon termination, you agree to pay Macadamian for all services performed up to the day of termination including work-in-progress and expenses incurred.

6. **Changes** - Throughout the course of the engagement, changes in the above engagement may be requested. Any request for change will only be effective when agreed to in writing.

7. **Limitation of Liability** - Our aggregate liability for all claims, losses, liabilities or damages in connection with this engagement whether as a result of breach of contract, tort or otherwise shall be limited to the value of this engagement. We will not be liable in any event for consequential, incidental, indirect or punitive exemplary or special damages, including any amount for the loss of profit, data or goodwill, whether or not the likelihood of such loss was contemplated.

8. **Warranty** - There is no explicit or implied warranty.

8.3 Additional Terms

Any travel or unspecified expenses incurred during the course of the engagement will be paid by *Patriot One* provided that prior written [email] permission was expressly given by *Patriot One*.

9 Governance

9.1 Changes in Scope

During the project, *Patriot One* or Macadamian may request additions, deletions, or modifications to the scope of the project or the services to be performed. Alternatively, an invalidation of a project assumption may have an impact on the project which may result in a change in scope, cost and or project schedule.

Macadamian shall have no obligation to commence work in connection with any change or continue with existing work (in the event of invalidated assumption(s)), until the effort, fee, and schedule impact is mutually agreed upon by the Parties in writing.

In the event that a change cannot be fully scoped at the outset of its identification, an interim change to perform additional discovery work shall be utilized.

9.1.1 Change Request Process

The following process will be followed if a change related to any exhibit or statement of work hereunder is required:
- "Change" refers to any changes in the original scope, deliverables, work activities, assumptions, responsibilities, terms of acceptance, communication, and costs defined herein.
- A Project Change Request (CR) will be the vehicle for communicating changes in scope to an agreed statement of work. The CR must describe the change, the rationale for the change and the effect the change will have on the project including the price, schedule and responsibilities of the parties.
- The designated Delivery Lead of the requesting party will review the proposed change and determine whether to submit the request to the other party.
- Unless a longer turnaround time has been mutually agreed upon, CRs raised by either party will be responded to by the other party within three (3) business days.
- Both Delivery Leads will review the proposed change and recommend it for further exploration or reject it.
  - Macadamian will specify any charges for such exploration. A CR must be signed by authorized representatives from both parties to authorize exploration of the recommended changes. No exploration work will start until the CR is signed by you.
  - **Macadamian will invoice *Patriot One* for any such charges.**
  - The exploration will determine the effect that the implementation of the CR will have on price, schedule and other terms and conditions of this master agreement or any exhibits or statements of work hereunder.
- A written change request must be signed by the Delivery Leads from both parties to authorize implementation of the changes. Until a change is agreed upon in writing, both parties will continue to act in accordance with the latest agreed version of the Agreement and any exhibits or statements of work hereunder.

9.2 Review Process of Written Deliverables

The review of the deliverables will use the following review process:
- An initial draft version of the Written Deliverables will be sent to *Patriot One* for initial review. *Patriot One* will have five (5) business days to review and submit all written feedback to us;
- A second, near-final version of the Written Deliverables will be sent to *Patriot One* for a last call of input. *Patriot One* will have five (5) business days to review and submit all written feedback to us;

○ This is the last opportunity to submit in-scope feedback;
● Upon receipt and inclusion of the near-final feedback, the Written Deliverables will be deemed, by us, to be complete. The completed Written Deliverables will be sent to *Patriot One* for acceptance.

9.3 Written Deliverables Acceptance Process

Upon completing work of a Written Deliverable, including the aforementioned reviews, it shall be submitted for acceptance to your Delivery Lead using the following process:
● The Project Lead will prepare an Acceptance Form using our template and submit it, along with the completed Written Deliverable to the Customer Delivery Lead;
● The Customer Delivery Lead will accept the deliverable within three (3) business days by signing and dating the Acceptance Form, or providing a cumulative list of written reasons for rejecting it and returning the Acceptance Form.
● Any feedback is treated as a Change Request and will be handled through the Change Request process.

9.4 Project Deliverable Acceptance

The Project Deliverable(s) shall be deemed accepted by us if one of the following occurs:
● The *Patriot One* Delivery Lead submits the signed Acceptance Form to the Macadamian Project Lead indicating acceptance of the Project Deliverable(s); OR
● There is no response from *Patriot One* Delivery Lead indicating acceptance or non-acceptance of the Project Deliverable(s) during a period of ten (10) business days from our last communication attempt, having made reasonable attempts in communicating with the Customer Delivery Lead and sending the Acceptance Form; OR
● The Project Deliverable(s) are being commercially used by the *Patriot One*.

9.5 Project Acceptance

During user acceptance phase (UAT) for a period of **10 business days** following design and development, *Patriot One* can report any issues that they find. Macadamian will fix all issues deemed ***Critical*** or ***Major*** (as defined in the Issue Severities section below).

For lower severity issues, or those reported after the project acceptance phase, Macadamian could provide support under a separate support/maintenance contract.

9.4.1 Issue Severities

Severity	Description
Critical	The issue affects critical functionality or critical data. It does not have a workaround. Example: Unsuccessful installation, complete failure of a feature, reproducible crash, loss of data or severe memory leaks
Major	The issue affects major functionality or major data. It has a workaround but is not obvious and is difficult. Example: A feature is not functional from one module but the task is doable if 10 complicated

	indirect steps are followed in another module/s.
Minor	The issue affects minor functionality or non-critical data. It has an easy workaround. Minor loss of function, or other problem, where workaround is present. Example: A minor feature that is not functional in one module but the same task is easily doable from another module.
Trivial	The issue does not affect functionality or data. It does not even need a workaround. It does not impact productivity or efficiency. It is merely an inconvenience. Example: Petty layout discrepancies, spelling/grammatical errors.

Contact Information and Signatures

For Macadamian Technologies, Inc	For Patriot One
Jim Stanish Email: jim@macadamian.com Tel: +1 (819) 772-0300	

IN WITNESS WHEREOF, the parties have executed this Agreement.

Macadamian Technolgies

By: *"James Stanish"*
Print: James Stanish
Title: CFO

Date: May 30, 2016

Patriot One

By: *"Kal Malhi"*
Print: Kal Malhi
Title: President

Date: May 30, 2016

Thank you.

Macadamian is a full-service software design and development firm that provides a complete range of highest quality usability, design, and software engineering services to industry leaders across North America. We care about the user and, as a result, create products that delight you and your customers. Our creativity and collaborative approach spark the ideas that ensure development of the best products. Our advanced, consistent experiences will be rapidly adopted by your desired audience right from the outset, because we think about the way your products are going to be received. The result? Your product will entice customers while standing out, maximizing your opportunity and delivering inspired results.

Visit macadamian.com
Call 1-877-779-6336

Macadamian Technologies Inc.
165 Rue Wellington
Gatineau, Quebec
J8X 2J3 Canada