Alberta Small Business Innovation and Research Initiative (ASBIRI) – Raytheon Cyber Challenge

Sponsored by Alberta Innovates and Raytheon Canada Limited

1.0 Program Overview

The Alberta Small Business Innovation and Research Initiative (ASBIRI) supports the commercialization of made-in-Alberta technologies by accelerating the development, demonstration, evaluation and adoption into the global market. This fund is part of the Ministry of Economic Development and Trade's mandate to strengthen Alberta's innovation ecosystem.

ASBIRI is a flexible sector agnostic platform program meant to catalyze unique partnerships between relevant stakeholders, industry leaders, and Alberta Small Medium Enterprises (SMEs) to create economic benefits for Albertans. These benefits include the:

- Promotion, growth, and entry of competitive Alberta companies and their technologies into the global market;
- Opportunities for economic diversification;
- Increased investment into Alberta's technology-based industries;
- Addition of new highly-skilled jobs;
- Establishment of valuable collaborations across industry, academia, and small business.

For more detailed information about the procedures and policies governing the ASBIRI program, click here. This Challenge is built on the foundation of the ASBIRI program guide; therefore it is highly recommended that you familiarize yourself with the program guide prior to applying.

2.0 Challenge Overview

Raytheon Canada Limited (RCL) is establishing an Alberta based cyber solutions centre with state-of-the-art cyber range capabilities focused on researching, assessing and validating the security and resilience of a wide range of technologies, infrastructures and systems. Successful SME participants in the ASBIRI challenge will leverage Raytheon's **Cyber Operations, Development and Evaluation (CODE™)** solutions centres and capabilities from Raytheon Canada Limited in Calgary with a potential for further collaborations with other locations in US and UK.

Challenge Stream 1: The primary area of focus of is to research and develop Critical Infrastructure Toolsets (CITs) and methodologies used to test and ensure the resiliency of existing and future operations-critical Information Technology (IT) and Operational Technology (OT) systems against cyberattacks.

Over the last few years, more and more IT being incorporated into OT. An obvious by-product of this convergence is the introduction of cyber threats heretofore the exclusive domain of IT systems now targeting OT. Significant steps have been taken to protect OT from such threats, but as the convergence continues, risks to OT will continue to increase. This challenge is offered to generate innovative methods and commercialize products to mitigate these risks and protect municipal, provincial and national critical infrastructures.

Challenge Stream 2: The secondary area of focus is to support the research into IT/OT and UAS technology convergence and integration across commercial, municipal and government agencies. This includes development of test procedures used to test, measure and confirm the security and resiliency of detection and monitoring systems such as a Low Power Radar (LPR) for protection of Unmanned Autonomous Systems (UAS) against cyberattacks.

As part of the diversification and expansion of industry in Alberta, a strong Unmanned Autonomous Systems sector is emerging. This innovative niche is expected to grow in the coming years because of its wide-ranging applications for military and commercial use especially when appropriately coordinated and linked to municipal and government's policies. UAS are employed in a variety of missions such as surveillance, law enforcement, oil and gas, agricultural, search and rescue, and payload delivery. Given the anticipated growth in use and complexity of UAS within Alberta, and across Canada, the likelihood of both vulnerabilities within UAS subsystems and threats to exploit those vulnerabilities will proportionately grow. In particular, the convergence of unmanned vehicular and aerial autonomous technology further enhances the risks associated with using these systems.

These challenge streams will engage a diverse set of Alberta based SMEs to provide innovative cyber security solutions which will augment current RCL Cyber Security capabilities for its Calgary (CODE™) Centre. The CITs developed by SMEs will target IT and OT systems intended for use across multiple Alberta Industries. The IT/OT CITs solutions are expected to include support of complementary and/or convergent capabilities, such as Industrial Internet of Things (IIoT) technologies for remote monitoring and control and Unmanned Autonomous Systems (UAS) technologies for perimeters and corridors monitoring and threat detection.

The cyber threat to IT/OT and UAS based systems carries significant implications for security and safety of critical infrastructure, social order, democracy, public health and economic development at all levels (municipal, provincial and national). Canada's market data and studies suggests the secure convergence of IT/OT and UAS is an economic imperative and this challenge would like to focus its solutions on novel methods and technologies capable of supporting The Government of Alberta's priorities which include Energy and GHG Mitigation, Health, Food & Agriculture, Fibre & Bioindustrial and Environment and Climate Adaptation.

Using the CODE™ Centre's advanced capabilities as the guidelines for establishing an IT/OT and UAS security and resilience testing regime, SMEs will target hardware, firmware and software for IT/OT sub-systems and UAS - both non-autonomous and autonomous - in order to provide assurance that identified risks are sufficiently mitigated and appropriate operating procedures are defined.

As part of the AI ASBIRI Cyber Challenge outcomes, RCL expects to sustain and grow a Cyber Security expert ecosystem in Alberta to bridge and fill our collective capability gaps with localized solutions. RCL will also leverage Challenge outcomes and relationships to pre-qualify select SMEs for our secure Supply Chain management in pursuit of future opportunities both in Canada and internationally.

Short-term, policy makers could analyze our results to guide harmonization of municipal, provincial and national critical infrastructure and UAS policies. Long-term, RCL will promote use of local and best in class CITs and methodologies, and prioritize selection of new or optimized CITs developed by participating SMEs. Additionally, RCL will provide SMEs with business development opportunities for additional innovation projects within our Network of CODE™ centres across US, UK and Australia.

2.1. Challenge Statement

2.1.1 Challenge Stream 1: Define, architect, build and validate a next generation state-of-the art IT/OT Critical Infrastructure Toolsets (CITs) for use in a Cyber Operations, Development and Evaluation (CODE™) Centre* (aka Cyber Ranges).

*A reference to a typical Cyber Operations, Development and Evaluation (CODE™) Centre is provided in Section 5 of this document.

2.1.2 Challenge Stream 2: Research and define areas of convergence and integration across IT/OT and UAS technologies. Develop test procedures for a UAS detection and monitoring tool sets using novel technologies such as a Low Power Radars with no moving parts. These UAS test procedures and tool sets tools sets should be defined for use in a (CODE™) Centre as well as a mobile deployable unit anywhere in Alberta.

Both streams could include SME's provision of professional services such as Cyber Security Architecting, Systems Engineering, Integration and Test engineering.

The proposed maximum financial contributions towards this Cyber Security Challenge are as follows:

Organization	Maximum Contribution
Alberta Innovates	$1.5M CAD
RCL	$500K CAD

Note that funding will likely be allocated across multiple projects and awardees under this Challenge.

2.2. Background: RCL's CYBER OPERATIONS, DEVELOPMENT AND EVALUATION (CODE™) CENTER - the ultimate proving ground for cyber critical infrastructure tools, systems and technologies.

RCL's cyber range envisioned for Alberta based industries helps customers test the resilience of critical technologies — with industry-leading agility, flexibility and scalability.

Alberta's industries and other select customers can:

- Customize sophisticated testing protocols in hours — not months;
- Expose systems and networks to realistic provincial and nation-state threats;
- Conduct force-on-force (attacker vs a corporate/government entity) exercises; and
- Evaluate the latest tools and techniques in cyber protection.

Customers can leverage RCL's Cyber Range or can work in collaboration with Academia, SMEs and RCL to build their own customized cyber range to suit their unique needs.

2.2.1 Typical Critical Infrastructure tools and methodologies for a Canadian RAYTHEON CODE™ Centre

The RCL Cyber Operations, Development and Evaluation (CODE™) Centre in Calgary, AB, Canada is envisioned as a state-of-the-art cyber range used to test existing and future mission-critical systems against cyber-attacks.

- **Test and evaluate advanced technologies** – The CODE™ Centre is used to test networks and systems by exposing them to realistic nation-state cyber threats in a secure facility with the latest tools, techniques and malware.
- **Conduct force-on-force cyber games/exercises** – The CODE™ Centre provides a simulated environment to conduct tests and rerun exercises to enhance cyber defense technologies and hone skills of cyber professionals.
- **Provide an engineering environment to integrate technologies** – The CODE™ Centre also offers a secure engineering environment for the integration of company-wide cyber capabilities, cybersecurity technologies, and customer and partner capabilities, along with the testing and demonstration of cyber technologies.
- **Provide cyber professional training** – Critical to the skills development of cyber professionals, Raytheon cyber ranges allow organizations to learn and practice with the latest techniques in cyber protection.

2.2.2 Versatile Cyber Environment with a focus on Alberta Industries

In order to set up a realistic exercise, cyber range operators can create an accurate replica of a system. The CODE™ Centre can emulate any size and kind of networked environment, including Power Grids, SCADA based OT systems, Water Supplies, Air Traffic Control or Security Operations Centers.

RCL's CODE™ Centre in Canada is currently focused on unique range automation software for IT/OT and UAS technologies where operators can rapidly set up a massive test range in hours or days, instead of months. Environments can be created to assess the destructive effects of attacks by nation states or sophisticated cyber criminals.

2.2.3 Interoperability with Raytheon's Global Network of Cyber Centers

A CODE™ Centre is part of Raytheon's network of cyber innovation and demonstration centers, around the world, that help customers rapidly pinpoint solutions to their most difficult and complex cyber challenges. Other Raytheon cyber centers in the network include:

- **Global Cyber Solutions Center (GCSC)** – A state-of-the-art environment that enables rapid assembly and assessment of technologies in addressing customers' operational cyber requirements. Built to be a modular, versatile security operation center (SOC), the GCSC can simulate real world events for training purposes. Based in Dulles, VA., close to Washington DC, it is geared towards international government and commercial customers.

- **Cyber Innovation Centre (CIC) in the U.K.** – Located in South-West (Cheltenham) England, the CIC provides development and test capability against current and emerging threats. Operating as a research, development and innovation hub, the CIC will enable Raytheon to work with its partners on projects and demonstrations while extending the company's deep cyber expertise to Europe and other international locations.
- **Raytheon Vulnerability Research Ranges** – Industry-leading vulnerability research expertise in Raytheon's Vulnerability Research Ranges in various locations are capable of conducting hundreds of millions of tests per week.

2.3. Technology Solution Characteristics

Challenge Stream 1: The Definition, Architecture, Build and Validation for IT/OT CITs, products and methodologies will enable security specialists, as well as system designers and architects, to design and implement next generation secure and resilient IT/OT technologies. Aspects of IT/ OT CITs and methodologies can include, but not be limited to:

1. Defence mechanisms that leverage machine learning and artificial intelligence algorithms for both insider and remote access threat assessments and attacks characterization
2. Cyber attribution tools and techniques
3. Cyber Security Operations Centres for critical infrastructure (IT/OT)
4. Intrusion Detection and Incident response
5. Tools for Digital Oilfield* use cases (*references available)
6. Fusion of analog and digital monitoring – new operational concepts
7. Cyberspace Visualization and real time Network Mapping and situation awareness
8. IT/OT protocols and anomaly-sensing technologies
9. Securing Supply Chain for operations critical and life saving systems
10. Proactive/dynamic computing systems defense, vulnerability research and assessments, reverse engineering and systems emulators and simulators, predictive data analytics
11. Advance techniques for industry specific persistent threats (including insider threats)
12. Secure AI for UAS using industry specific Observe, Orient, Decide, Act loops (algorithms)

Challenge Stream 2: The research of areas of convergence and integration between IT/OT and UAS and development of testing procedures for UAS detection and monitoring tolls will provide data necessary to enable municipalities and governments' policy planners, security specialists as well as system designers and architects to design and implement integrated, secure and resilient IT/OT and UAS technologies. Aspects of UAS that would be targets of testing can include, but not be limited to:

1. Location tracking assurance - onboard global positioning system as well as alternate geo tracking mechanisms – resistance to signal spoofing, for example
2. UAS to ground station command and control (C2) links – resilience from jamming, signal hijacking and man-in-the-middle attacks leading to hijack of the UAS, for example

3. Strength of assurance of the of the robotic and AI technology used within the autonomous elements of the UAS
4. Security / resilience of telemetry and sensor/payload communication links
5. Resistance to or susceptibility to denial of service attacks of C2 and Cloud links
6. Security / resilience of smart charging systems
7. Strength of authentication and authorization controls, both the ground station and the UAS
8. Effectiveness of collision avoidance systems
9. Software assurance validation
10. Software / firmware patching
11. Vulnerability assessments of security controls, procedures and training
12. Advance techniques for persistent threats (including insider threats)

3.0 Industry Partner Overview

3.1. Raytheon's Global Network of Cyber Operations, Development and Evaluation (CODE™) Centers

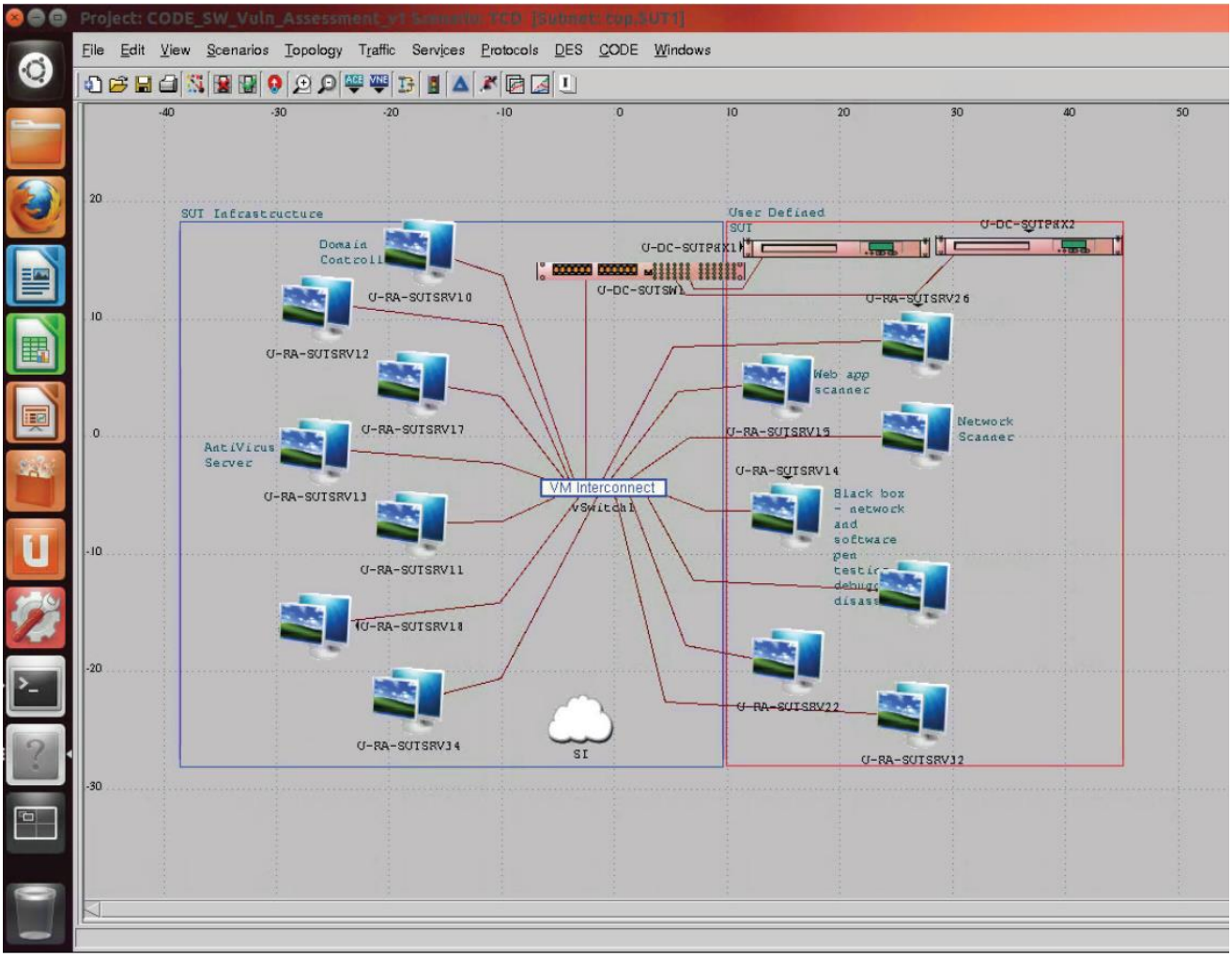
Raytheon is building a fit-for-purpose CODE™ Centre in Calgary, Alberta, Canada to provide a fully functional testing centre, which includes cyber ranges using modular components to meet the mission-unique and complex needs of our customers.

In the massively complex and chaotic environment of cyberspace, owners and defenders of interconnected networks require controlled environments to accurately and safely assess their defenses and effectiveness of day-today operations. RCL plans to implement a fit-for-purpose cyber range capability which provides a customized virtual environment that enhances our customers' cyber operations, training and cyber security assessment capabilities.

Our CODE™ Centre Cyber Range capabilities will provide a broad set of tools and a unique range automation capability that will help strengthen the stability, security and performance of cyber infrastructures and IT/OT and UAS based systems used by large global companies, SMEs and government agencies.
In order to be responsive to emergent customer needs, RCL's cyber range architecture supports the ability to rapidly set up and tear down test environments of moderate to high complexity (hundreds of nodes to tens of thousands and up) within hours to as many as a few days. Repeatability is a key concern with regard to test agility and consistency and our cyber range design allows for the retention of emulated environment designs (storage, hardware, and proven procedures) and a means to reconstitute these designs in a repeatable, error free manner.
As scale increases, automation and artificial intelligence becomes increasingly important. RCL's custom ability to automate deployment of connectivity, storage, operating systems and applications allow

range operators to create large environments in as little as a few hours or in a matter of several days, where in the past equivalent manual preparation activities could extend for weeks to months. At its core, our advanced automation technologies provide a flexible layer-one switching infrastructure for a consistent and accurate automated topology deployment. It also provides an accelerated means of loading representative operating systems and application stacks. RCL's cyber range architecture is scalable from as few as sixteen ports to over ten thousand and from a few nodes to hundreds of thousands of virtual and/or real nodes.

RCL's cyber range architecture ensures reliable separation of test environments from range administrative and management functions. It also enables a hardware-in the-loop testing capability allowing real systems to interact with virtual stimuli; full network tap capability allowing the capture of any traffic in an event; and the aggregation, filtering and replication of that tapped traffic.



Raytheon's custom range automation software facilitates rapid creation of a test infrastructure topology without the need to physically patch equipment every time.

Raytheon also has a set of 40+ fully defined Standard Operating Procedures that can be easily adapted to our customers' unique cyber range requirements. Raytheon's cyber range architecture is extensible to allow for simulation of friendly systems, mission services and networks ranging from a single

physical host to tens of thousands of virtual hosts running in a cloud computing environment. The cyber range is also designed to support future connectivity with external entities such as other cyber ranges to carry out cooperative testing at Internet scale.

The Raytheon Cyber Range delivers the scalability, extensibility, flexibility and automation needed today by companies and organizations to maintain their edge in protecting their critical information and enterprise services.

For video overview of a typical Raytheon Cyber Range please watch the video found here (CTRL click): Raytheon Cyber Range

4.0 Process

4.1. Challenge Phases

The application process for this Challenge will take place in three phases:

Stage I: Expression of Interest

This stage is open to the public and will require Applicants to submit an Expression Of Interest (EOI). The EOI will be used to assess and identify opportunities that align with the challenge, have a clear competitive advantage, have a viable path to market and will have a significant impact in Alberta within a reasonable timeframe.

Application area and Challenge Stream must be identified in the EOI (Stream 1 and/or Stream 2).

Stage II: Full Project Proposal

This stage is by invitation only, with successful participants selected from Stage 1. Applicants will be required to submit their up-to-date year-end financial statements, a 5-year financial forecast and a basic business plan.

Stage III: Project Work Plan and Budget

This stage is by invitation only, with successful participants selected from Stage 2. Applicants will be required to submit a proposal outlining the development/demonstration of their technology in collaboration with the appropriate subcontractors, as well as letters of support (if applicable).

4.2. Evaluation Criteria

Broadly, the evaluation criteria will focus on the opportunity, potential impact and feasibility:

- ✓ The Opportunity.
  - **Market.** The optimal solution and provider will be strongly positioned to address a clearly characterized and quantifiable market that is significant both in Alberta and globally.
  - **Technology.** The optimal solution will be sufficiently developed to ensure a timeline to field demonstration of less than 3 years.
  - **Business.** The optimal solution will be commercialized by an Alberta SME with the experience, expertise, planning and financial resources to realize the potential of the technology as well as the capacity to support the product through its lifetime (design, parts, maintenance, training, etc.).
- ✓ The Impact.
  - **Alberta.** The impact to Alberta will need to be significant, measurable and timely. This impact may be related to social well-being and/or economic development through new venture creation, production facilities and/or direct supply-chain growth and maturation.
  - **SME.** Growth is expected in the form of increased revenue, new export market/customer acquisition, recruitment and retention of highly skilled workers and follow-on investment.
- ✓ Project Feasibility.
  - **Outcomes.** The project must be outcome-focused with appropriate milestones, timelines, and resource allocations.
  - **Support.** The project must have the appropriate supports in place, including partners, personnel, infrastructure and access to sufficient financial resources needed to ensure success.