WATCHHub Business Case: Modernizing Wildlife and Public Health Surveillance

Contents

Simulation Document Overview

Simulation Context:

This document is part of a fictional simulation designed to model a public-sector response to a virus outbreak. The scenario assumes the existence of three independently funded, fragmented data-collection entities—**IoT wildlife sensors**, **field researchers**, and **regional lab clinics**—alongside a central coordinating body, the **Wildlife Analysis and Technology Center for Health (WHATCH)**

While WATCH serves as the central coordinating body for wildlife health data, its current operations are hampered by outdated, siloed processes. Data sharing across field teams, IoT devices, and regional labs remains clumsy and manual—**severely limiting** the ability to detect and respond to zoonotic threats in real time.

Purpose of This Document:

This document represents a **realistic business case**, framed for public-sector decision-makers, proposing a **cloud-based modernization solution** to unify these systems and processes. It serves as the **first step in the broader simulation journey**, leading to the technical architecture, implementation plan, and evaluation documents that follow.

1. Executive Summary

Project Overview

The *Wildlife Analysis and Technology Center for Health* (**WATCH**) is the central coordinating body responsible for collecting, analyzing, and distributing wildlife health intelligence. However, its current operational model relies heavily on **siloed**, **manual processes** across three independently funded data collection entities: field teams, IoT-based environmental monitoring, and regional laboratory clinics.

These disconnected workflows result in **severe risk to public heath** due to ***delayed data sharing***, ***reduced operational agility***, and ***costly, convoluted manual processes*** that *strain both time and resources*. Staff and stakeholders alike face ongoing frustration with **inefficient handoffs**, **slow insight generation**, and **limited ability** to act on the data being collected.

This business case proposes a **centralized data coordination platform** to significantly **reduce risk to the public, lower costs**, improve responsiveness, and enable the WATCH mandate.

Strategic Importance

The current state imposes a **high administrative burden**, delays **responsiveness** to outbreaks, introduces **avoidable latency**, and limits **cross-agency coordination**. This business case proposes a **modern, integrated solution** that:

- **Streamlines** data sharing across collection entities
- **Cuts costs** by eliminating manual data processing and redundant tasks
- **Reduces** manual handoffs and duplication
- **Improves** response agility and insight generation
- **Supports** cross-jurisdictional collaboration

This is a *business modernization initiative*, with **digital tools enabling smarter coordination** across agencies.

Funding Request Summary

This business case requests funding to launch a **phased rollout** of a modern data coordination platform under the WATCH mandate. The requested investment will support:

- **Solution design** and **enterprise architecture**
- **Deployment** of secure, scalable ingestion and analytics workflows
- **Cloud infrastructure, platform services,** and **operational support**
- **Stakeholder onboarding,** training, and change management

This initiative represents a multi-agency modernization effort with **immediate gains in responsiveness** and long-term **reductions in operational cost, duplication, and delay**. The funding enables WATCH to shift from reactive coordination to **proactive, insight-driven response**—at a fraction of the current administrative overhead.

2. Problem Statement

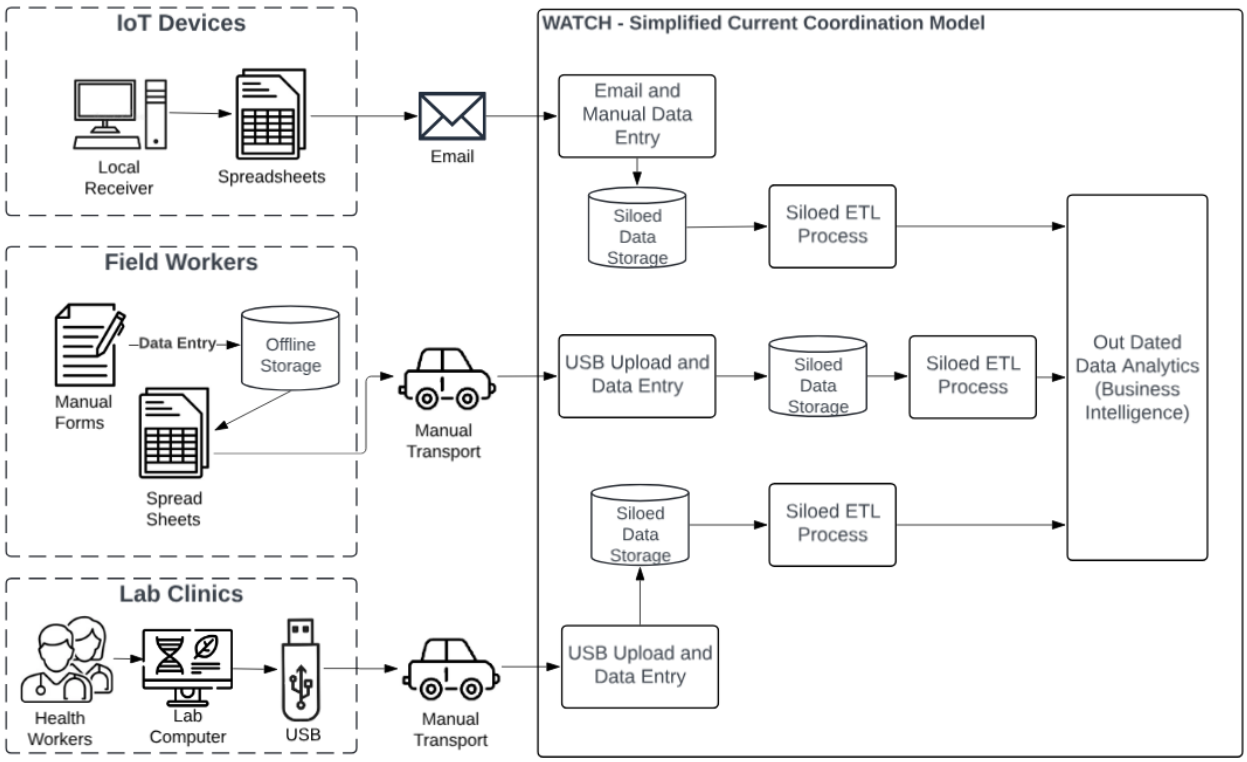
Current Landscape (Existing Systems)

Wildlife health data is currently collected by three independently funded entities:

- **IoT-enabled monitoring devices**, which store data locally or on third-party platforms
- **Field teams**, who rely on manual forms, spreadsheets, and offline data collection
- **Regional laboratory clinics**, which store biosample data locally and transfer USB drives manually

Each entity performs a critical function, but they operate in silos—using disconnected tools and manual processes to share data with WATCH. Coordination occurs through **email, USB drives, and manual data entry**, resulting in **duplicated effort, delayed insight, and limited situational awareness**.

WATCH, while responsible for oversight, **lacks an integrated platform** to unify these inputs or support real-time response.



Key Challenges and Limitations

- **Manual Processes**: Data is shared through email, spreadsheets, or physical transfers—introducing delays, errors, and administrative burden.
- **Lack of Real-Time Insight**: Data often arrives late or incomplete, limiting situational awareness during emerging events.
- **Duplicated Effort**: Each agency maintains its own systems and workflows, resulting in costly redundancy and resource strain.
- **Siloed Systems**: No centralized access point for stakeholders to collaborate or analyze cross-source trends.

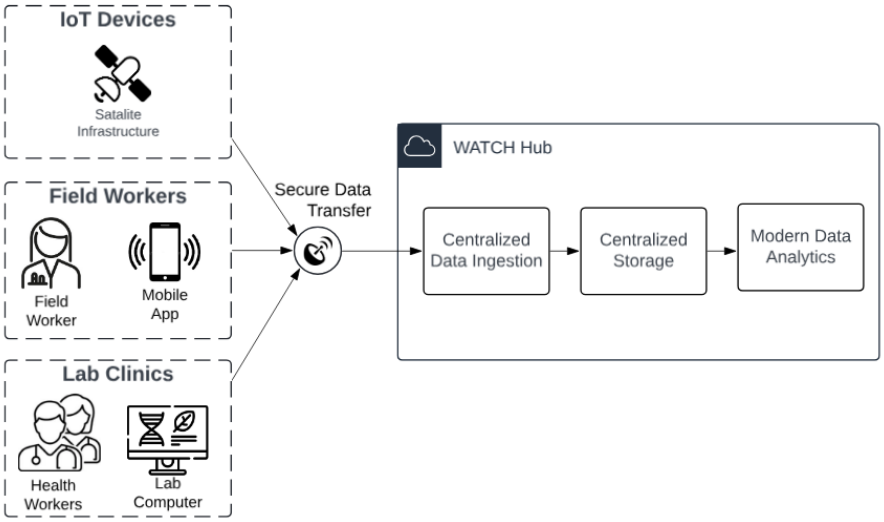
Risks of Maintaining Status Quo

- **Delayed Response to Public Health Threats**
  Fragmented systems delay detection and coordination—risking late response to emerging zoonotic outbreaks.
- **Unsustainable Operational Costs**
  Manual processes require increasing time and staffing to maintain. The cost of maintaining the status quo continues to rise without delivering improved outcomes.
- **Operational Collapse Under Pressure**
  Manual workflows and limited staff capacity cannot scale in this crisis. Surges in the virus is overwhelming the system.
- **Erosion of Stakeholder Confidence**
  Teams are fatigued by inefficient processes. Continued strain leads to burnout, disengagement, and staff turnover.
- **Missed Early Warnings**
  Without integrated data, key signals in wildlife or human health may go unnoticed until consequences escalate.
- **Reputational and Compliance Risk**
  Slow or inconsistent response exposes the program to public criticism and potential failure to meet policy obligations.

3. Proposed Solution: WATCHHub Platform

Vision and Scope

The proposed solution is a phased implementation of **WATCHHub**—a centralized coordination platform designed to securely consolidate wildlife health data from field teams, IoT devices, and lab clinics.
WATCHHub will replace fragmented, manual workflows with a single, automated pipeline for **data ingestion, storage, and analysis**, enabling real-time insight and faster response across agencies.
Serving as the digital backbone of the WATCH program, the platform will reduce duplication, streamline collaboration, and significantly improve the government's ability to identify and respond to emerging wildlife and public health risks.



Core Capabilities

WATCHHub will provide:

- **Secure, real-time data ingestion** from field teams, IoT devices, and lab clinics
- **Automated data processing** to eliminate manual entry and reduce duplication
- **Centralized storage and structured access** to unify data across sources
- **Integrated dashboards and reporting tools** for real-time insight and early detection
- **Role-based access controls** to support collaboration across agencies
- **Scalable design** to support high-volume periods and future program growth
- *Future-ready features*: AI-driven trend detection and automated alerting (optional next phase)

These capabilities will reduce operational burden, improve cross-agency coordination, and enable faster, evidence-based public health interventions.

Target Users and Stakeholders

WATCHHub is designed to support a broad range of users across the program, including:

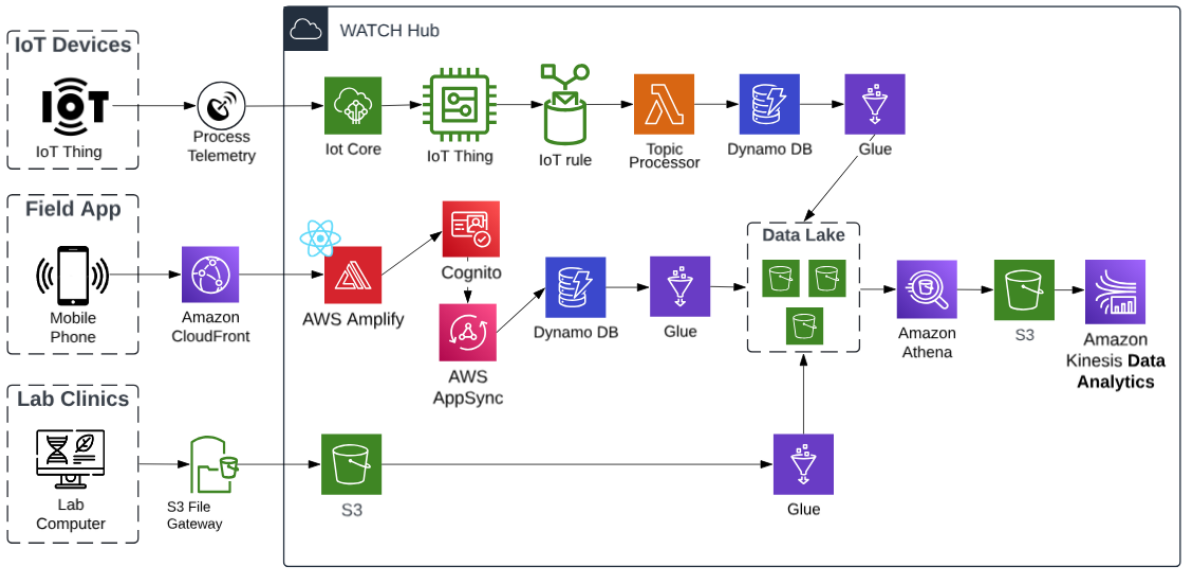
- **Field teams** collecting observational and environmental data
- **Laboratory personnel** processing bio-samples and submitting test results
- **Program analysts and epidemiologists** interpreting data trends and generating insights
- **WATCH coordination staff** managing workflows, alerts, and operational oversight
- **Partner agencies** with limited or role-specific access for inter-agency collaboration

Each group will benefit from **tailored access controls and interfaces**, ensuring secure, relevant, and user-friendly participation across all areas of the program.

4. Architecture Overview

AWS Cloud Architecture – Data Ingestion to Analytics

The following diagram presents a high-level proposal for a potential AWS-based solution. It is not intended to provide an exhaustive list of services or architectural components, but rather to illustrate the overall end-to-end flow — from data ingestion through transformation to analytics — across IoT devices, field applications, and lab systems.



This architecture is designed to fulfill the WATCH Hub's central mission: enabling **real-time, cross-agency insight and response** by integrating fragmented data into a unified platform.

IoT Devices (Remote Sensors)

- Wildlife-mounted GPS collars and environmental sensors collect time-stamped telemetry and environmental data.
- Data is transmitted securely via AWS IoT Core and funneled into the platform using managed rules for preprocessing or direct storage.
- Lightweight messaging protocols (e.g., MQTT) ensure reliable low-bandwidth transmission from remote regions.

Field Applications (Mobile App)

- Field staff collect observational and environmental data using mobile apps connected through AWS Amplify.
- User authentication is handled by Amazon Cognito, ensuring secure, role-based access.
- Field inputs are submitted via AppSync (GraphQL), triggering real-time writes to DynamoDB and optionally stored in S3 for structured analytics.

Lab Systems (Test Results & Diagnostics)

- Regional clinics upload structured test data through secure interfaces or batch uploads.
- Ingested data flows into AWS S3 buckets for staging, then moves through AWS Glue ETL pipelines for transformation and metadata tagging.
- Structured outputs land in the core data lake, where they can be queried or joined with field and IoT datasets.

Backend Services & Analytics Layer

- Transformed datasets are made queryable via Amazon Athena, allowing analysts to generate insights across the entire wildlife health landscape.

- For real-time processing needs (e.g., anomaly detection or early warning), Amazon Kinesis Data Analytics is available.
- Role-based dashboards can be delivered to WATCH analysts and partner agencies through secure endpoints.

— *See Appendix A for detailed AWS Service descriptions.*

Together, these services form a fully serverless, secure, and highly available pipeline — from field-level data capture to enterprise-grade reporting and analytics.

Security, Privacy, and Compliance Measures

AWS offers industry-leading security and compliance capabilities, including robust tools like **Secrets Manager, IAM, Amazon Cognito, CloudWatch**, and **CloudTrail** — all designed to protect sensitive data, manage access, and ensure continuous monitoring and auditability across the platform.

Additionally solution is built with strong safeguards to ensure data privacy, security, and alignment with public-sector standards.

- **Privacy by Design**: Sensitive health data is protected at every stage, from capture to storage to analysis. All components are selected and configured with privacy in mind.
- **Secure Access**: Only authorized users can access the system, and access is based on roles and responsibilities. Identity management ensures the right people see the right data — and nothing more.
- **Data Protection**: All information is encrypted during transfer and when stored. Data from the field, clinics, and IoT devices is handled with care and stored securely in compliance with government expectations.
- **Monitoring and Auditability**: The system keeps full logs of access and changes, supporting transparency, traceability, and accountability.
- **Canadian Data Residency**: All data remains within Canadian borders and is processed in the Canada (Central) AWS Region.
- **Compliance-Ready**: The architecture is aligned with FOIPPA and leverages AWS services that meet industry and public sector security certifications.

5. Business and Public Health Impact

Benefits to Wildlife Health Monitoring

The WATCH Hub strengthens the core mission of wildlife health monitoring by transforming fragmented, manual inputs into a unified, real-time intelligence system. This modernization supports:

- **Earlier Detection of Anomalies** – Patterns in animal health data can be identified sooner through integrated surveillance
- **Improved Data Quality and Continuity** – Centralized ingestion ensures more valuable insights can be drawn to support proactive interventions, shape evidence-based public health policies, and allocate resources more effectively during emerging threats.

- **Cross-Agency Visibility** – Wildlife, lab, and field stakeholders access the same data, improving coordination and response
- **Long-Term Monitoring and Research** – Structured, analyzable data sets support trend analysis and conservation planning.

Public Threat Mitigation

An integrated surveillance system like WATCHHub dramatically improves the province's ability to anticipate, contain, and respond to zoonotic threats before they reach the public domain. By consolidating fragmented workflows, it shifts the paradigm from reactive crisis management to proactive public health defense.

- **Rapid threat detection** through real-time signals from field teams, environmental sensors, and lab diagnostics.
- **Targeted intervention**, including the ability to detect and neutralize infected wildlife before cross-species transmission occurs.
- **Improved public safety coordination**, enabling faster, evidence-based decisions across multiple agencies.
- **Minimized outbreak escalation**, thanks to reduced latency, clearer visibility, and shared situational awareness.

Time and Cost Efficiencies

The WATCHHub platform introduces immediate and long-term operational savings by eliminating redundant tasks, accelerating workflows, and reducing resource dependency across disconnected entities.

- **Elimination of manual data entry** across field, lab, and reporting teams — reducing labor hours and human error.
- **Reduced duplication of effort**, especially where the same data is currently re-entered, revalidated, or reprocessed across silos.
- **Streamlined coordination**, minimizing delays caused by email chains, manual file transfers, or unclear task ownership.
- **Lower administrative overhead** through automated workflows, centralized tracking, and built-in audit trails.
- **Reduced reliance on ad hoc tools** like Excel, email, or SharePoint for data compilation and reporting.
- **Faster data availability**, enabling quicker decisions and limiting the cascading costs of delayed interventions.
- **Better staff utilization**, allowing highly skilled analysts and health professionals to focus on value-added tasks rather than manual reconciliation.
- **Cloud-native architecture**, removing the need for large capital investments in infrastructure or on-prem support.
- **Scalability without proportional costs**, allowing the system to absorb more data and more users without linearly increasing expenses.
- **Improved procurement efficiency**, thanks to modular solution design and reusable platform components.

6. Implementation Plan

Phased Roadmap

Phase	Estimated Duration	Description	Key Activities & Deliverables
1. Stakeholder Engagement & Reference Architecture	**Week 1–2**	Establish shared understanding and foundational alignment across all three data collection entities.	• Multi-agency engagement sessions• Define governance model• Approve Reference Architecture document
2. Detailed Solution	**Week 3–4**	Translate the reference	• AWS services mapped to functional flows (IoT, Field,

Architecture		architecture into a detailed, implementable cloud-native design.	Lab)• Data flow diagrams• Security & IAM considerations
3. Proof of Concept (PoC)	**Week 5–6**	Build a testbed to validate architecture assumptions, tools, and user flow feasibility.	• Simulated data ingestion from IoT, mock field app, and lab inputs• Working prototype dashboard• Stakeholder feedback sessions
4. Minimum Viable Product (MVP)	**Week 7–12**	Build out core data ingestion pipelines across each stream. Focused on functionality over polish.	• **IoT Pipeline:** – AWS IoT Core, S3, Kinesis, Glue, Athena• **Field App Pipeline:** – Amplify, Cognito, AppSync, DynamoDB, S3• **Lab Data Pipeline:** – API/S3 ingestion, Glue ETL, cross-source join
5. Pilot Deployment (Targeted Region)	**Week 13–16**	Live deployment in one selected region or use-case scenario with end-user training.	• Full-stack onboarding of real users• Collect usage metrics and pain points• Refine authentication, dashboards, field flows
6. Full Deployment (All Entities)	**Week 17–24**	Gradual rollout to remaining stakeholders, including training and support.	• Configure IAM and multi-tenant access• Production dashboards finalized• System adopted as central reporting hub
7. Optimization & AI Enablement	**Week 25–28**	Improve data quality, reduce latency, and explore predictive AI layers.	• Integrate anomaly detection / early warnings• Implement cost optimization (e.g., lifecycle policies)• Finalize sustainment and ops governance

Team and Roles

Role	Key Responsibilities
Program Sponsor / Executive Lead	Provides overall oversight, funding support, and strategic alignment with public health objectives.
Project Manager	Oversees timelines, resources, and stakeholder coordination; ensures milestones are met across entities.
Enterprise Architect	Defines the overarching architecture and ensures technical cohesion across IoT, field, and lab pipelines.
Solution Architect	Designs AWS-based solution components; translates business needs into secure, scalable system architecture.
DevOps Engineer / Cloud Specialist	Implements and maintains cloud infrastructure (CI/CD, monitoring, automation, security hardening).
IoT Integration Engineer	Handles sensor onboarding, MQTT configuration, edge data preprocessing, and AWS IoT Core integration.
Mobile App Developer	Develops and maintains the field data capture interface (Amplify, AppSync, offline capabilities).
Data Engineer	Designs data pipelines, schema transformation (Glue), and ingestion logic for all three data sources.
Data Analyst / Epidemiologist	Supports dashboard design, analytics validation, and ensures data outputs are decision-useful.
Security & Privacy Officer	Ensures data protection, compliance with privacy legislation (e.g., FOIPPA), and security audits.
Change Management & Training Lead	Drives user onboarding, training, support materials, and adoption strategies across agencies.
Business Leads – IoT, Field, Lab	Act as subject-matter experts for their respective domains and validate system effectiveness from the ground level.

Success Metrics / KPIs

To ensure the success of the WATCHHub platform, the following strategic indicators will be tracked during development and initial rollout:

Category	Key Performance Indicator (KPI)
Timeliness	Reduction in time from data capture to usable insight (e.g., field report to dashboard)
Cost Efficiency	Reduction in manual processing hours and duplication across teams
Data Completeness	% of incoming records successfully integrated from all 3 entities (IoT, Field, Lab)
User Adoption	Active usage rate across key user groups (field workers, analysts, labs)
Response Agility	Decrease in time-to-action during simulated or actual outbreak scenarios
Security & Privacy	Compliance with FOIPPA standards and zero critical security incidents during pilot

7. Budget and Resource Requirements

Funding Request Breakdown (infra, dev, data ops, etc.)

The proposed budget supports a rapid, phased implementation of the WATCHHub platform. Funding is allocated across core workstreams to ensure scalability, security, and measurable outcomes.

Category	Description	Estimated Cost (CAD)
Solution Architecture & Planning	Enterprise architect, tech leads, stakeholder workshops, documentation	$250,000 – $400,000
Application Development	Frontend + backend devs, UI/UX, API and dashboard build	$600,000 – $900,000
Data Engineering & Integration	Ingestion pipelines, ETL, schema design, API integration	$400,000 – $650,000
Cloud Infrastructure Provisioning	Platform setup, secure VPCs, managed services, scaling configuration	$150,000 – $250,000
Security & Compliance	Identity, RBAC, FOIPPA compliance, audit systems	$100,000 – $200,000
Testing & Pilot Deployment	QA engineers, test environments, early pilot support	$100,000 – $150,000
Training & Change Management	Documentation, onboarding, cross-agency support	$75,000 – $120,000
Project & Product Management	PMO, Product Owner, coordination, governance	$200,000 – $300,000
Contingency (10–15%)	Scope flexibility, unexpected cloud usage, delays	$200,000 – $300,000

Total Estimated Cost: **$2.1M – $3.3M CAD**

Note: Exact funding values to be finalized following stakeholder alignment and cloud pricing model estimation. Budget request reflects a timeboxed, 8-month deployment cycle.

AWS Services Operating Cost Forecast

(Based on phased MVP → full deployment across IoT, field apps, and lab ingestion pipelines)

Service	Purpose	Est. Monthly Cost	8-Month Total
AWS Fargate	Serverless backend containers (e.g., data processing APIs)	$150–$300	$1,200–$2,400
AWS Glue	ETL and schema management	$300–$600	$2,400–$4,800
Amazon Athena	Querying data in S3 Data Lake	$100–$250	$800–$2,000
Amazon S3	Scalable data storage and Data Lake	$80–$150	$640–$1,200
DynamoDB	Low-latency storage for real-time records	$100–$200	$800–$1,600
AWS IoT Core	Streaming telemetry from remote devices	$100–$250	$800–$2,000
AWS AppSync	GraphQL APIs for field app and lab comms	$100–$200	$800–$1,600
Amazon Cognito	User identity, RBAC, secure access	$50–$100	$400–$800
CloudWatch + SNS	Monitoring, alerting, logging	$50–$150	$400–$1,200

Other (API Gateway, Lambda, misc.)	Glue code, triggers, and small services	$100–$200	$800–$1,600

Contingency & Buffer (10–15%) | $300–$600/month | $2,400–$4,800 |
Estimated Total AWS Spend (8 Months):
$11,440 – $23,000 CAD *(assuming moderate usage and phased adoption)*

8. Risk Mitigation Strategy

Technical Risks

WATCHHub's architecture must manage complex, distributed data pipelines across multiple domains. This introduces risks related to system integration, scaling under load, and data loss in edge scenarios. These risks are mitigated through modern serverless design, modular deployment, and robust AWS infrastructure.

Risk	Description	Mitigation Strategy
Integration Complexity	Challenges in harmonizing data across disparate systems (IoT, field, labs)	Leverage serverless AWS architecture and schema normalization via AWS Glue; phase-based onboarding allows staged validation
Scalability Issues	Increased data volume during outbreaks could strain system performance	Architecture is designed with horizontal scalability; AWS auto-scaling and load balancing built-in from inception
IoT Connectivity Failures	Remote devices may lose connectivity, creating data blind spots	Use AWS IoT Device Shadow for offline buffering and re-sync, plus redundant local data capture on edge devices
Vendor Lock-in Concerns	Heavy reliance on AWS services	Use of standard APIs and modular design to enable service abstraction and cloud portability if needed

Data Privacy and Regulatory Compliance

As a public-sector platform handling potentially sensitive wildlife and zoonotic data, WATCHHub must meet FOIPPA requirements and inter-agency privacy standards. The solution embeds compliance through access controls, encryption, and transparent governance by design.

Risk	Description	Mitigation Strategy
FOIPPA Non-Compliance	Mishandling of personal or sensitive data violates BC's Freedom of Information and Protection of Privacy Act	Enforce strict RBAC via Amazon Cognito, encrypt data in transit and at rest, and apply automated audit trails using AWS CloudTrail
Cross-Agency Data Sharing Sensitivities	Variability in data access permissions across field, lab, and oversight entities	Role-based access configuration per user group, legal data-sharing agreements, and transparent consent practices embedded in onboarding
Unauthorized Access or Breaches	Security breach risks due to centralized data platform	Secure network design (private VPCs), AWS-native threat detection (e.g., GuardDuty), real-time monitoring with CloudWatch/SNS alerts

Sustainability and Operational Continuity

The long-term success of WATCHHub depends on stable operations, funding, and cross-agency adoption. To prevent project drift or obsolescence, the roadmap includes phased ROI, documentation, capacity building, and resilient infrastructure planning.

Risk	Description	Mitigation Strategy
Lack of Sustained Funding	Long-term success depends on budget continuity	Modular delivery enables phased ROI demonstration; cost forecasting includes 12-month post-launch ops for budgeting clarity
Knowledge Transfer Gaps	Risk of institutional memory loss or staff turnover	Deliverables include technical documentation, onboarding packages, and internal capability uplift via training sessions

Cloud Service Disruptions	Reliance on third-party cloud infrastructure	Utilize AWS high-availability zones, automatic failover, regular backup procedures, and SLAs for uptime guarantees

9. Conclusion and Call to Action

Why This Project Now

The threat of zoonotic disease is no longer hypothetical — it is accelerating. Wildlife surveillance systems are currently fragmented, slow, and manually burdened, leaving gaps in early detection and public safety response. WATCHHub presents a time-sensitive opportunity to unify these efforts under a modern, scalable, and secure platform. The technology is ready. The foundational work has already begun. Now is the moment to act.

Alignment With Strategic Priorities

WATCHHub aligns directly with government and public health mandates around:

- **Proactive health protection and outbreak response**
- **Digital modernization of field and lab systems**
- **Data-driven decision-making and inter-agency collaboration**
- **Improved transparency, efficiency, and cost control**

This project is not just an IT upgrade — it's a public safety and operational modernization imperative.

Call to Action

We are seeking:

- **Executive endorsement** to move forward with phased implementation
- **Funding allocation** to support the 8-month build and rollout cycle
- **Partnerships across agencies** to align operational workflows and ensure long-term sustainability

The path forward is clear. The risk of waiting is greater than the cost of action. Let's build WATCHHub — together.

Ask: Funding, Endorsement, or Partnership

We are requesting:

- **Funding** to support the full 8-month delivery of WATCHHub, covering infrastructure, development, integration, and sustainment.
- **Executive endorsement** to proceed with the phased roadmap, including stakeholder alignment, solution architecture, and deployment.
- **Cross-agency partnership** to ensure seamless coordination between IoT, field, and lab entities, and to maximize the public health impact.

This is a unique opportunity to modernize wildlife and zoonotic surveillance at scale — with clear, measurable outcomes in operational efficiency, public safety, and cost control. Your support is the key to realizing it.

Appendix A

AWS Service	Role in Architecture
IoT Core	Ingests telemetry data from remote wildlife monitoring devices
AWS Amplify	Hosts the field app and connects it securely to backend services
Amazon Cognito	Manages user authentication and fine-grained access control
AWS AppSync	Enables real-time, serverless GraphQL communication between field app and backend

DynamoDB	Stores structured field and IoT data with millisecond latency
Amazon S3	Stores raw files, lab results, and analytical outputs
AWS Glue	Performs data extraction, transformation, and schema enrichment before analytics
Amazon Athena	Executes SQL-based ad hoc queries directly on the S3-based data lake
Kinesis Data Analytics	Powers near-real-time streaming analytics and alert generation