# **AWS Imagine Grant 2025 – Pathfinder Proposal**

**Project Title:** The Guardian Project: AI-Powered Policy Repository and Generative AI for Automated Policy Synthesis & Security Analysis

**Applicant Organization:** Cyber Institute

Project Overview  
The Guardian Project is an AI-driven, cloud-native policy repository that leverages **generative AI** to automate policy synthesis, cybersecurity analysis, and global AI governance recommendations. This project will revolutionize how policymakers, industry leaders, and researchers develop, compare, and stress-test AI and quantum-related regulations.

The system will utilize **Amazon Bedrock and SageMaker** to generate, analyze, and refine policy documents dynamically, ensuring unbiased policy recommendations optimized for **cybersecurity, ethical AI governance, dual-use prevention, and compliance with emerging regulations.**

The Guardian Project aligns with AWS's Pathfinder initiative by integrating **generative AI** to create **scalable, repeatable solutions** that directly impact AI and cybersecurity policy development at a global level. By leveraging AWS cloud infrastructure, this initiative will enhance efficiency in policy decision-making, strengthen compliance mechanisms, and proactively address gaps in global AI governance frameworks.

Problem Statement  
Governments, corporations, and research institutions lack a **centralized, unbiased AI-driven policy repository** that can:

* **Compare AI & cybersecurity policies globally** in real time.
* **Automate policy generation** to ensure alignment with emerging cybersecurity and AI governance standards.
* **Use stress-testing simulations** to validate policy effectiveness under different threat scenarios.
* **Predict and mitigate dual-use risks** where emerging technology could be weaponized or misused.

The current **fragmented** and **manual** policy development process leaves critical security gaps, particularly in the wake of rapid AI and quantum technology advancements. **Failure to address these gaps has led to severe consequences, including:**

* **Cambridge Analytica Scandal (2018)** – Inadequate data privacy policies allowed AI-driven profiling to manipulate elections, exposing weaknesses in global digital governance frameworks.
* **Deepfake Disinformation Campaigns (2024 US Primaries)** – The absence of robust AI-generated content regulations led to mass voter suppression through AI-generated robocalls impersonating political figures.
* **EU AI Act Implementation Challenges (2023-Present)** – Despite being one of the first comprehensive AI governance laws, slow enforcement and loopholes have allowed non-compliant AI models to persist in high-risk industries.
* **Quantum Cryptography Risks (Ongoing)** – Nations and corporations are struggling to prepare encryption standards for post-quantum threats due to a lack of coordinated policy efforts, leaving financial and government institutions vulnerable to future decryption attacks.
* **AI and Autonomous Weapons Development (Ongoing)** – Without standardized, enforceable global policies, AI-powered weapons systems continue to advance, raising ethical and security concerns regarding their deployment in conflict zones.

These examples demonstrate the **urgent need for a generative AI-powered policy platform** that can rapidly **analyze, synthesize, and stress-test** regulations before real-world vulnerabilities emerge. The Guardian Project is positioned as a critical initiative to address these challenges through a **data-driven, AI-enhanced policy management system** that fosters transparency, efficiency, and cross-sector collaboration.

# **Proposed Solution**

**Generative AI-Powered Policy Repository**  
The Guardian Project is in the **pilot deployment phase**, transitioning from **patent-pending innovations** to real-world implementation. AWS support will enable scaling, optimization, and refinement of the platform to maximize its impact. This initiative builds upon **ongoing research, AI governance best practices, and policy compliance strategies**, ensuring a well-grounded and actionable framework.

**Key Components:**

* **AI-Powered Policy Generation & Summarization:**
  + **Amazon Bedrock** will generate structured AI policy drafts by analyzing global policy datasets.
  + **Amazon SageMaker** will refine policies by comparing them against compliance benchmarks and ethical AI principles.
  + **AWS CodeWhisperer** will assist in automating policy coding and enforcement mechanisms.
* **AI-Driven Cybersecurity & Ethics Gap Analysis:**
  + **Natural Language Processing (NLP)** models in **SageMaker** will assess global AI regulations and detect cybersecurity or ethics gaps.
  + **Generative AI** will **suggest missing cybersecurity measures,** ensuring AI policies meet global standards (e.g., GDPR, NIST, OECD AI guidelines).
  + **Predict and mitigate dual-use risks** by analyzing historical patterns of technological weaponization and generating **early-warning policy recommendations.**
* **AI-Powered Policy Stress-Testing & Risk Simulation:**
  + **AI-based sandboxing environment** will simulate the **real-world impact** of AI policies under different **cybersecurity attack scenarios**.
  + **AWS High-Performance Computing (HPC)** will analyze policy effectiveness at scale.
  + **Generative AI-powered simulations** will predict potential dual-use scenarios, allowing policymakers to adjust regulatory frameworks proactively.
* **AI-Powered Recommendations & Continuous Learning:**
  + **Amazon Bedrock** will generate **policy improvement recommendations** based on historical AI regulatory outcomes.
  + A **reinforcement learning model in SageMaker** will continuously refine AI-generated policy drafts.
  + **Automated policy synthesis** will combine the **best components** of various global policies, ensuring real-time adaptability and alignment with emerging challenges.
  + **Shortens the policy norm and adoption cycle** by **using generative AI to anticipate and predict issues**, ensuring greater collaboration across sectors and governments.

# **SMART Metrics & Success Milestones**

* **Specific:** Deploy AI-powered policy repository to **15+ national AI regulatory bodies** within 18 months.
* **Measurable:** Reduce **manual policy analysis time by 60%** using AI automation.
* **Achievable:** Perform **5,000+ AI policy stress-test simulations annually** to prevent regulatory loopholes.
* **Relevant:** Increase **policy harmonization accuracy by 40%** using AI-driven synthesis.
* **Time-Bound:** Enable **automated compliance monitoring for at least 10 international AI governance organizations** within the first two years.

Long-Term Sustainability & Partnerships  
Sustainability is a key consideration for the Guardian Project. The following strategies will ensure its long-term viability:

* Monetizing the repository through **enterprise subscriptions for compliance automation**, while keeping access free for governments and non-profits.
* Continuous AI-driven policy synthesis updates to adapt to **new global regulations and security threats**.
* Establishing **strategic collaborations with AI ethics groups, regulatory bodies, and think tanks** for policy data contributions and validation.
* Letters of support from policymakers and industry stakeholders, reinforcing industry-wide interest and adoption potential.

Conclusion  
The Guardian Project is a **pilot-ready initiative** moving from **patent-pending research to large-scale implementation**, using AWS generative AI to transform AI policy generation and cybersecurity analysis. By leveraging **Amazon Bedrock, SageMaker, and CodeWhisperer,** this initiative will create a **global, scalable AI-driven policy repository** that ensures AI governance is **transparent, efficient, and adaptable to emerging threats**. AWS funding will accelerate this transition, enabling real-world deployment and establishing a sustainable, forward-looking policy management framework.

This initiative aligns with AWS’s mission to support **AI-driven solutions for critical global challenges**, making it a perfect fit for the **Pathfinder – Generative AI** award.

# **Contact Information**

Andrew Vance, PhD  
Cyber Institute