The Cybersecurity Readiness Podcast Series

Episode Title	AI Security in the Public Sector: Balancing Innovation and Risk
Podcast Series	The Cybersecurity Readiness Podcast Series https://www.cybersecurityreadinesspodcast.com/
Host and Producer	Dave Chatterjee, Ph.D. https://dchatte.com
Guest	Burnie Legette, Director of IoT and AI at Intel Corporation and former professional football player
Summary Pitch	In this episode, Dr. Dave Chatterjee is joined by Burnie Legette, Director of IoT and AI at Intel Corporation and former professional football player. Their conversation explores the evolving landscape of AI deployment within the public sector, with a particular focus on the security challenges and governance strategies required to harness AI responsibly. Drawing on his cross-sectoral experience, Burnie offers insights into the cultural, technical, and ethical nuances of AI adoption. Dr. Chatterjee brings in his empirically grounded Commitment-Preparedness-Discipline (CPD) cybersecurity governance framework to emphasize the importance of planning, transparency, and stakeholder engagement.
Discussion Highlights	**Burnie's Unconventional Journey** From top-ranked running back at the University of Michigan to leading AI initiatives at Intel (2:00–3:53) **Lessons from the Gridiron** Discipline, preparation, and passion are vital in both sports and technology (3:58–5:03)

	AI in Private vs. Public Sectors Private sector prioritizes speed and market entry; public sector prioritizes risk management and regulation (9:34–12:44) **AI Attack Surface** Every stage—from data collection to user interface—presents potential vulnerabilities (10:34–12:44) **Security as a Core Innovation Driver** Effective AI strategies embed cybersecurity from the outset, not as an afterthought (14:40–15:03) **Collaborative Development** Success depends on early involvement of business, legal, IT, and security teams (21:33–23:03) **Data Governance and Auditability** Secure AI begins with high-quality data and ends with transparency and explainability (23:04–30:03) **Human Oversight and Risk Assessment** High-risk use cases require a balanced mix of automation and human judgment (24:17–25:49) **The Coke Machine Analogy** Transparency builds user trust—people trust what they can see and understand (28:16–30:03)

	Culture Change Precedes Tech Adoption For AI to succeed, organizations must first embrace a culture of ethical, secure innovation (32:14–35:06)
Actionable Recommendations	1. **Embed Security into AI Strategy**: Treat cybersecurity as a foundational component of AI innovation, not a separate concern. 2. **Establish Cross-functional Teams Early**: Involve business, legal, and cybersecurity leaders in the AI planning and development process. 3. **Prioritize Data Governance**: Implement policies ensuring high-quality, protected, and well-governed data across storage, transit, and use. 4. **Develop Transparency Mechanisms**: Ensure that AI decisions can be audited, explained, and understood—especially in high-impact sectors. 5. **Conduct Risk Assessments**: Classify AI use cases by their risk levels and apply varying degrees of human oversight accordingly. 6. **Foster a Culture of Adoption**: Encourage upskilling and address AI-related fears through education and behavioral nudges. 7. **Build Modular, Adaptable AI Platforms**: Design AI systems that can evolve with changes in regulation and risk environments.
Time Stamps	00:00 – Introduction to host and show 00:49 – Guest introduction: Burnie Legette 02:00 – Burnie's personal and professional journey 03:53 – Transferable lessons from sports 05:03 – The CPD framework and passion 07:18 – Motivation vs. passion in career choices

	08:18 – Framing AI innovation in public sector 09:34 – Public vs. private sector AI experience 10:34 – AI risk vectors and vulnerabilities 12:44 – Intel's data-centric security model 14:51 – Strategic alignment of AI, business, and security 17:31 – Public sector examples and unintended consequences 19:30 – Incentives, mandates, and coordination 21:33 – Importance of cross-functional collaboration 23:04 – Oversight and governance 24:17 – Risk-aware platform design 25:37 – Parenting metaphor for AI maturity 28:16 – Transparency and the Coke machine analogy 29:51 – Explainability and responsible use 32:14 – Final reflections on AI culture and security 34:54 – Closing thanks 35:01 – Outro and disclaimer
Memorable Quotes/Statements	**Burnie Legette:** • *"Security is part of your innovation—it's not a tension. It should be planned from the onset."* • *"The technology will only go as far as the security will enable it."* • *"There has to be a level of transparency—users need to understand how decisions are made."* • *"Before technology adoption, there needs to be a culture of adoption."* **Dr. Dave Chatterjee:** • *"We must make mindful use of technology, not mindless use."*

	• *"Security, business, and AI strategy must be integrated from the very beginning."* • *"Cybersecurity is everybody's business. It can't just rest with the developers and defenders."* • *"Unless the leadership is committed to AI security, that mindset won't filter across the organization."*