National Information and Communication Technology Company Limited

Building a Secure and Resilient Public Sector for the Future

Feature Address by
Senator the Honourable Dominic Alexander Smith
Minister of Public Administration and Artificial Intelligence

Inaugural iGovTT National CyberDrill

Date: 22 July 2025

Building a Secure and Resilient Public Sector for the Future

Feature Address by Senator the Honourable Dominic Alexander Smith – Minister of Public Administration and Artificial Intelligence

Inaugural iGovTT National CyberDrill

The Honourable Roger Alexander, Minister of Homeland Security; Dr. Inshan Meahjohn, Chief Executive Officer of iGovTT; distinguished leaders from our public and private sectors; members of our protective services; and future leaders in technology.

A very good morning to you all.

"Sonae areba urei nashi" - "If you are prepared, you need not worry" - Japanese proverb

Today's Inaugural National CyberDrill is not merely a technical exercise. It is a critical milestone in our government's foundational agenda: to build a modern, efficient, and trusted public service for the 21st century. As we accelerate our transition to digital-first governance, to improve how we serve our citizens and how our country competes on the world stage, we must ensure the bedrock of this transformation is unshakeable. That bedrock is cybersecurity.

I commend iGovTT for spearheading this vital initiative, and I thank all our institutional partners and every participant for your commitment. Your presence here signals a shared understanding of the task before us.

For too long, the conversation around cybersecurity has been confined to the realm of IT specialists. I am here today to assert that cybersecurity is no longer just a technical necessity – it is a core pillar of public trust and good governance.

In our private lives, we have embraced technology to connect with family, to conduct business, to learn, and to create. Citizens now rightfully expect this same seamless, digital-first experience from their government. But with every new online service we launch, we enter into a new dimension of the social contract. We are asking citizens to place their sensitive personal and commercial data into our custody. Our ability to protect that data is the modern currency of public trust. Studies have shown a direct correlation: when citizens trust in the security of digital government platforms, they are far more likely to use them, leading to greater efficiency and national development. The integrity of our digital public infrastructure is therefore paramount to maintaining the confidence of the people we serve.

To secure that trust, we must strengthen our capabilities from within. This CyberDrill is a direct and vital investment in our most valuable asset: our public officers. We are empowering our Ministries, Departments, and Agencies with the skills, awareness, and collaborative mindset needed to defend our digital estate. Initiatives like this, which bring together expertise from across the public and private sectors, are precisely the kind of cross-functional collaboration we must foster. It is how we build

sustained, unified efforts that move us beyond reacting to threats in isolation, towards a posture of collective resilience.

As we look to the future, we cannot ignore the force multiplier that is Artificial Intelligence. As the Minister responsible for both Public Administration and AI, I see its dual nature with absolute clarity. We are aware that AI presents a new class of threat, enabling adversaries to craft more sophisticated and automated attacks. We are also aware that it offers our most powerful defensive tools. The global market for AI in Cybersecurity is projected to exceed $60 billion USD by 2028, for a simple reason: AI can analyse billions of data points in real-time to detect anomalies and predict threats in a way no human team ever could, on their own. It allows us to move from reactive defence to predictive defence.

My vision is for Trinidad and Tobago's public sector to become a leader in the responsible and ethical adoption of AI – not only to streamline services, but to build more intelligent and resilient cyber defence systems that anticipate and neutralise threats before they can cause harm.

And so, my call to action today, particularly to my colleagues in the public service, is to champion a culture of holistic security. This culture begins with embedding security-by-design as a foundational principle, ensuring that security is not an afterthought but is woven into the very fabric of every new process and public service from its inception.

This proactive foresight, however, is only one half of the equation. It must be complemented by our readiness to respond. A truly resilient public service not only builds strong digital architecture – it constantly hones its incident response capabilities, the very skills you are sharpening here today, ensuring that when an incident occurs, we are prepared to act with speed, precision, and unity.

Let us leave here today committed to building a public service that is not only digital-first, but security-first. Let us build a government that is agile, resilient, and worthy of the enduring trust of the people of Trinidad and Tobago as we lead our nation confidently into the digital future.

Thank you.