

**MESSAGE FOR 20TH ANNUAL HEALTH, SAFETY,
SECURITY AND ENVIRONMENT (HSSE) CONFERENCE AND
EXHIBITION
NOVEMBER 8-9, 2016**

Salutations

Thank you, Mr Chairman.

Let me begin by thanking the American Chamber of Commerce of Trinidad and Tobago for inviting me to address its 20th Annual Health, Safety, Security and Environment (HSSE) Conference and Exhibition. I extend my congratulations to you on hosting the largest local gathering of professionals from the private and public sector in this field for another successful year.

I am particularly pleased by the choice of topic which you have asked me to address today - "ICT Resilience - Protecting the Government's IT Infrastructure".

You should know that ICT is central to this government's plan to refocus and re-energise this economy as it prepares for diversification. Let me begin by letting you in on a little secret. Whenever you drive along St Clair Avenue, you should take a long look at the building that houses the Office of the Prime Minister.

That building, originally designed by architect Mark Raymond to house the Ministry of Information, was designed in the form of a microchip. It was opened in 2006 as we began to focus on the information era. That building, now occupied by the Office of the Prime Minister, is recognition of the importance to this government, and the Manning administration under which it was built, of the ICT driven economy.

It is during that period that much of our ICT infrastructure began to be formalised. Today according to the World Economic Forum's ICT Readiness Sub-Index on Infrastructure, we are ranked 35th in the world.

The challenge facing us now is to build on this ICT infrastructure to transform the society and the economy.

This government is committed to expanding the country's information economy. To do so will require not just robust physical infrastructure but also human capacity development and innovation. All of these constitute critical success factors in achieving meaningful and long-term transformation of our country.

And we have been making strides in this regard.

As the Ministry of Planning and Development is assiduously advancing work on the elaboration of the National Development Plan, *Vision 2030*, the Ministry of Public Administration and Communications is concomitantly seeking to revise the National ICT Plan to ensure that the necessary alignments are made to Trinidad and Tobago's wider development goals.

In this regard, in June 2016 we convened a committee of National ICT experts, both locally and regionally based, to:

- review and assess the accomplishments gained and challenges experienced under past national ICT plans namely, *fastforward I* and *smarTT*; and
- chart a path forward with a new plan that emphasizes meaningful ICT usage and uptake and greater ICT innovation for the benefit of our citizens and for increasing economic prosperity.

Currently, this National ICT Plan Working Group has started to develop a first working draft of the revised ICT Plan in keeping with the five broad development goals of Vision 2030.

Once reviewed by the Ministry and Cabinet, the National ICT Plan will be put forward for wide-reaching public consultation before being approved and implemented.

Re-constitution of the e-Business Roundtable

In 2016, the Trinidad and Tobago e-Business Roundtable celebrates 10 years of laudable work championing the greater use of ICTs in the private sector and providing Government with policy inputs on key ICT initiatives.

Established in July 2006, this public-private partnership of leaders in the ICT industry, business sector, public sector and academia works to advance economic diversification by advocating for the extensive use of technology, particularly in the non-energy sector.

The Trinidad Guardian on May 27, 2016 reported on a study conducted by Mastercard on the use of electronic transactions in Trinidad and Tobago. According to the study T&T's economy can grow by 3.5 per cent if the country increased electronic payments by 30 per cent in a four-year period.

While we support the private sector, we acknowledge that government has a critical role to play in making this goal a reality. That is why, I am able to give the commitment today that this government is committed to the full implementation of the Electronic Transactions Act 2011.

The Act will provide not just for government payments but also has the potential to increase government earnings. Full implementation will mean that local entrepreneurs can also establish systems to receive international payments electronically. This can lead to a whole new e-business industry creating a new foreign exchange source.

With this mind the Ministry has since re-constituted the e-business roundtable to expedite implementation. The committee is chaired by Mrs. Glynis Alexander-Tam, representative of the electronic payments industry and co-chaired by Mr. Simon Aqui, representative of American Chamber of Commerce. The Ministry of Public

Administration and Communications serves as both a member of the committee as well as provides it with secretariat support. Now armed with its renewed mandate, the Committee is expected to convene regular meetings as early as this month.

I have already identified to the chairman, Mrs Alexander-Tam, that the acceleration of the adoption of electronic payments must be a major priority on the Roundtable's agenda.

We remain committed to building our ICT infrastructure. In July 2016, this Government, in an attempt to ensure that our citizens have greater access to the Internet launched a free WI-Fi service aboard thirteen PTSC buses. This initiative, TTWIFI, will provide an opportunity for citizens utilising the public transport system to access online services conveniently.

Additionally, through the deployment of the Government's e-Taxes initiative, citizens filing their taxes now have the option to do so online.

It is my intention, through the National ICT Company Limited, better known as iGovTT, and other stakeholders, to ensure the implementation of systems that will support the operation of ICT infrastructure and programmes across Government agencies.

Our e-Government service portal, *ttconnect*, managed by iGovTT continues to improve the delivery of government services to residents and organisations. We acknowledge that citizens desire even more convenient services in real time and we are working on meeting these expectations.

Ladies and Gentlemen, as the Minister responsible for ICT, I recognise that trust and public confidence are critical to advancing the national ICT agenda and to expanding the online economy. Of the examples, that I

will provide, an underlying success factor which is often regulated to second place, is that of an enabling environment for ICT. Yet, it is the area for which the Government has primary responsibility.

Key components include the policy, legal and regulatory structures that allow for predictability, transparency, awareness, dependability and security. To this end, I am pleased to inform you that we are currently addressing key pieces of legislation including the amendment of the Telecommunications (Amendment) Bill and the Data Protection Act.

As we seek to expand our reach in the realm of ICT, the issue of protecting Government's IT infrastructure becomes even more critical. The Government is the single largest collector and processor of information in our country as well as a repository of information related to governance, the country's assets and the personally identifiable information of our citizens. In our digital age, unauthorised access to this information is a major

risk that has to be effectively managed through proper access, control and monitoring practices and procedures.

Today, the Government is faced with the challenges that come with rapid technological developments. Existing security measures and requirements often become obsolete as new threats arise with the development in technology.

Cognisant of the need to ensure that our critical infrastructure is protected, in 2015, Cabinet directed that iGovTT conduct a thorough and in-depth review and analysis of the security requirements of the Government's networking environment.

In compliance with this Cabinet directive, a strategic plan entitled "The ICT Security Strategy for the Government of the Republic of Trinidad and Tobago, 2017 to 2019" and its accompanying Implementation Plan, was developed by iGovTT.

iGovTT is responsible for the Government's centralised ICT infrastructure and is an agency under the umbrella of the Ministry of Public Administration and Communications.

The ICT Security Strategy for the Government addresses not only endpoint protection in the Government's significant inventory of desktops and laptops, but also addresses the comprehensive need for appropriate ICT policies, procedures and governance.

This ICT Security Strategy seeks to safeguard our information and information systems from unauthorised access and use. It serves to identify, design and implement appropriate security controls in order to maintain confidentiality, integrity and availability as required.

Significantly, it will define, establish and implement an Information Security Governance Framework for our

Government and by extension, the people of Trinidad and Tobago.

In moving forward, a vital element of our security strategy, is the establishment of an Information Security Governance Committee, which focuses not only on the existing infrastructure but on the dynamic nature of the world of ICT security, its risks and threats.

Work is proceeding apace on the establishment of this committee which will require a whole of government approach that includes representatives of the Ministry of National Security, the Ministry of Public Administration and Communications, iGovTT and other key stakeholders.

The Government's second strategic objective entails developing and implementing an information security programme. This initiative entails the creation of a comprehensive programme to manage the many elements of Government information security, including: identity and access management through a centralised

and streamlined access control solution, defining our risk management processes as well as our risk mitigation and risk treatment plans, continuous threat and vulnerability assessments and annual penetration tests of our Ministries, agencies and GovNeTT.

This holistic approach will also include the development and implementation of our remediation plans, our business continuity management plan and our central information security monitoring capability.

In ensuring that our Government has a consolidated and reportable ICT security risk profile, we must also ensure that proper documentation practices exist, our data classification system is properly developed and used and that our Government has a working Information Security Programme and Enterprise endpoint protection.

As we seek to make proactive risk management our modus operandi, endpoint security protection becomes all the more significant. In our digital age, the

Government requires enterprise-wide, standardized, endpoint security products and services to combat growing, dynamic threats against its expanding inventory of desktops and laptops.

These threats include spam, malware, spyware, phishing, password stealers and identity theft in addition to newly emerging threats. The selected information security, endpoint solution must offer 24/7/365 real-time security analytics, threat detection and remedial response across the disparate networks of the government.

With this in mind, in mid-2016, a security health check was conducted on all devices utilising our current endpoint protection solution to determine the security risks and vulnerabilities that exist, including virus infections, use of outdated and unsupported operating systems and outdated endpoint client protection versions that are prone to virus infections.

Furthermore, the implementation of controls and counter-measures integration within the Government's ICT environment will inform the decision-making process and effectiveness of the security governance framework.

This will be achieved through IT and Assurance audits and information security controls reviews. By prioritising security incident management, we can manage security events more efficiently and effectively, thereby minimising the impact of security incidents.

Initiatives that support this objective, such as enhancing existing incident response or incident handling capabilities through training, and through developing security incident management procedures, will help the Government recover its information assets in the wake of any catastrophic event.

The Government will also be emphasising security awareness training and education for all employees and Government leaders so that they may become more

aware of security threats in the current environment. This will also help the Government to obtain a better understanding of its ICT security risk profile and work towards transforming the Government's environment to a security aware culture.

In essence, the Government's ICT security strategy emphasises confidentiality of information, integrity of information and information systems, availability of information to authorised parties, appropriate authentication and identification of users and proper ICT and security risk management, deployed at all levels of the ICT infrastructure.

In closing, I wish to emphasise this Government's commitment to developing our digital Government services to facilitate greater efficiency and convenience to our citizens and residents.

Every time you drive or walk pass the microchip façade that houses the Office of the Prime Minister, let it be a

reminder that this government is conscious and committed to protecting your information security.

I thank you and I now welcome any questions you may have.



Presenters at the session on "Security: ICT Vulnerability and Business Risks" at the AMCHAM TT 20th Anniversary HSSE Conference and Exhibition, November 8, 2016, Hyatt Regency, Port of Spain.

From l-r: Kathy West, Systems Analyst, Indiana University of Pennsylvania (IUP), Eric Gaull, Vice President, BDA Global, the Honourable Maxie Cuffie, Minister of Public Administration and Communications, Nirad Tewarie, CEO AMCHAM TT (moderator) and Ben Dadson, Systems Analyst, IUP.