



Ministerial Statement

By

The Hon. Michael Weeks, JP, MP
Minister of National Security

Cybersecurity Workshop

June 3rd, 2022

Mr. Speaker, you will recall from the 2021 Speech from the Throne that data is the new oil, and Bermuda must ensure that our cybersecurity defenses are adequate to defend our island from dangerous online actors.

We committed to introduce a CyberSecurity Act which will establish minimum standards for cybersecurity for critical assets such as energy supply, telecommunications, water infrastructure and government data.

Mr. Speaker, I am pleased to inform this Honorable House that work is underway on the Legislation which I intend to table this calendar year.

Mr. Speaker, the Legislation is only a part of our Cybersecurity Strategy. Global trends and reports indicate that the number and severity of cyber-incidents affecting individuals and organisations across nations will grow. This, coupled with the rapidly evolving cyber-threat landscape means that Bermuda needs to identify and classify cyber threats, enhance management of cyber-threats and provide support to

organisations across all sectors on how to manage these threats particularly our critical national infrastructure.

Mr. Speaker, this week a cybersecurity workshop is being provided to both Government and private sector stakeholders with responsibility for critical national infrastructure.

Mr. Speaker, the five day workshop, which ends today, is being presented by two experts from the International Telecommunications Union; Mr. Marwan Rached and Mr. Pablo Palacios. The ITU is the United Nations' specialised agency for information and communication technologies and we are very fortunate to have these two subject experts on Island to present the workshop. The workshop will assist us in building national cyber resilience and the protection of critical information infrastructure.

Mr. Speaker, the workshop is also focusing on the functions and role of a National Cyber Security Incident Response Team or CSIRT to improve our ability to protect, detect and respond to cyber threats. This includes providing technical training for Government Cyber Incident responders and the setting up of:

- a threat sharing platform;
- security monitoring systems;
- an incident management system; and
- a digital forensics system.

Mr. Speaker, the ITU emphasize that at the national level, cybersecurity is a shared responsibility which requires coordinated action for prevention, preparation, response, and incident recovery on the part of government authorities, the private sector and civil society.

Mr. Speaker, this workshop is part of our commitment to meet that responsibility including partnering with the private sector in protecting our critical national infrastructure from the rapidly evolving cyber-threat.

Thank you, **Mr. Speaker.**