WRITTEN QUESTION TO THE CHIEF MINISTER
BY DEPUTY H.L. JEUNE OF ST. JOHN, ST. LAWRENCE AND TRINITY
QUESTION SUBMITTED ON MONDAY 8th JULY 2024
ANSWER TO BE TABLED ON TUESDAY 16th JULY 2024

Question

"In relation to cyber security risks, will the Chief Minister advise –

(a) what measures and Government funding exists to protect public services, Government departments and States Members;
(b) what training and support is provided to those using States of Jersey provided products and applications; and
(c) which, if any, UK bodies the Government is working with in relation to managing these risks?"

Answer

a. The internal response to cyber security risks for Government provided systems and services is managed by the Government of Jersey and led by Modernisation and Digital (M&D).

As part of increasing the cyber protection for Government departments and public services delivered by the Government of Jersey, there has been investment in Cyber Security through capital funding as part of the Cyber Security Programmes, as detailed in recent Government Plans. This investment has delivered improvements, including a Security Operations Centre, monitoring systems events and risk assessing alerts for remedial action.

Operational day-to-day technical protection measures for Government of Jersey systems are provided by the Modernisation and Digital (M&D) technical operational teams and their work in ensuring sufficient security measures are in place across Government devices. These technical protection measures include firewalls, encryption, anti-virus and anti-malware software to name a few. These are supplemented by the Security Standards and Policies which are in place across Government public services and extend to subjects such as physical security and the role of all staff in maintaining security.

The Jersey Cyber Security Centre (JCSC) is an arm's length capability which promotes and improves the Island's cyber resilience, supporting the critical national infrastructure, public services, business communities and citizens to prepare, protect and defend Jersey from cyber threats both at home and abroad.

b. As part of the Government of Jersey's corporate statutory and mandatory staff training, which is available to States Members, there is a Cyber Security focussed training module which covers important information related to keeping data safe, security awareness in the office, good password practice and safe ways of using email. The training in place is in addition to the Security Standards and Policies referred to earlier in the response which provides an additional layer of support to public services which are in place across public services and extend to subjects such as physical security and the role of all staff in maintaining security.

c. The Jersey Cyber Security Centre works closely with the UK National Cyber Security Centre, which is the UK Government body which provides advice and support to the public and private sector for the avoidance of computer security threats. In addition, Government departments and other public bodies work closely with their UK counterparts. For example, the Jersey Competition and Regulatory Authority (JCRA) and the Department for the Economy work closely with NCSC and the UK telecommunications regulator OFCOM on matters of telecoms security. JCSC, States of Jersey Police and the Financial Intelligence Unit - Jersey (FIUJ) also work and share intelligence with their UK counterparts on wider matters related to national security, cybercrime, counter terrorism and computer fraud. JCSC also engages with international bodies such as the Forum of Incident Response and Security Teams (FIRST) of which NCSC is also part and co-operates directly with NCSC on cyber incident response.