

**MINISTRY:**

**STATE SECURITY:**

# REPUBLIC OF SOUTH AFRICA



**NATIONAL ASSEMBLY**

**QUESTION FOR WRITTEN REPLY**

**QUESTION NO.:** **1508**

**Inkosi R N Cebekhulu (IFP) to ask the Minister of State Security:**

Whether her department has taken any steps to ensure that the cybersecurity of the Republic is not compromised in the wake of the COVID-19 pandemic during which there had been a worldwide rise in cybercrimes and ransom attacks; if not, what is the position in this regard; if so, what are the relevant details? NW1715E

**REPLY**

The SSA through its National Communications provides the following as measures and steps to ensure that Information and Communications Technology (ICT) Security or cyber security in organs of state is maintained.

Provision of ICT Security Solutions and services to organs of state for protecting and securing electronic systems:

Rendering periodic and on-demand Information Assurance services and continuous monitoring services to clients and identified Critical Information Infrastructure:

* + Conducting technical Vulnerability and Risk assessments to identify and report on common critical vulnerabilities affecting Organs of state.
  + Continuous monitoring of ICT Security network infrastructures and systems of Organs of state in order to provide proactive alerts and warnings that help to protect the systems before harm.
  + Provision of Incident response to compromised systems of organs of state to mitigate risks and deploy measures to avoid recurrence of ICT security and Cyber-attacks and incidents.
  + Provision of cyber security awareness.

SSA National Communications is also busy with the review of the Cyber Security Strategy to improve the security and resilience of national infrastructures and services. The strategy establishes a range of national objectives and priorities that should be achieved in a specific timeframe.

The review/finalisation of the Cybercrimes and Cybersecurity Bill:

* to define offences and impose penalties that have a bearing on cybercrime
* to criminalise the distribution of data messages that are harmful
* to provide for interim protection order
* to further regulate jurisdiction in respect of cybercrimes
* to further regulate the powers to investigate cybercrimes
* to further regulate aspects relating to mutual assistance in respect of the investigation of cybercrime
* to provide for the establishment of a 24/7 Point of Contact
* to further provide for the proof of certain facts by affidavit
* to impose obligations on electronic communications service providers and financial institutions to assist in the investigation of cybercrimes
* to report cybercrimes
* to provide for the establishment of structures to promote cybersecurity and capacity building
* to regulate the identification and declaration of critical information infrastructures and measures to protect critical information infrastructures
* to provide that the Executive may enter into agreements with foreign States to promote cybersecurity
* to delete and amend provisions of certain laws
* to provide for matters connected therewith.