**PARLIAMENT OF THE REPUBLIC OF SOUTH AFRICA**

**NATIONAL ASSEMBLY**

**WRITTEN REPLY**

**QUESTION NO: 1648**

**DATE OF PUBLICATION: 09 JUNE 2017**

**QUESTION PAPER NO: 21**

**DATE OF REPLY:**

**Mrs MR Shinn (DA) to ask the Minister of Telecommunications and Postal Services:** Whether all the computer operating software and application licenses governing all end-user workstations and servers installed and maintained by the State Information Technology Agency include regular updates to address the system flaws to prevent malicious attacks; if not, why not; if so, (a) what operational protocols have been put in place to ensure these changes are implemented and (b) how are these updates audited?   NW1854E

**REPLY:-**

**I have been informed by SITA as follows:**

SITA has instituted a process to ensure that all system flaws identified are remediated (patch management) by implementing the latest operating system and application software updates on all workstations and servers installed and maintained by SITA to prevent any known security breaches.

1. Updates are verified by conducting bi-weekly vulnerability assessment scans in consultation with the various service environments to update operating system and application software (code changes) where deemed necessary. Where updates are released by the suppliers of the software, it is also implemented after it has been tested.
2. The environment is audited by the SITA Internal Audit by conducting vulnerability assessments and penetration testing. This is complimented by external penetration testing on an ad hoc basis. Furthermore, the Auditor-General also performs penetration testing and vulnerability scans on a selected sample of the infrastructure installed and maintained by SITA on an annual basis.

**Approved/Not Approved**

**---------------------------------**

**Dr Siyabonga Cwele, MP**

**Minister of Telecommunications and Postal Services**

**Date:**