

**Ministry**

**Employment & Labour**

**Republic of South Africa**

Private Bag X499, PRETORIA, 0001. Laboria House 215 Schoeman Street, PRETORA Tel: (012) 392 9620 Fax: 012 320 1942

Private Bag X9090, CAPE TOWN, 8000. 120 Plein Street, 12th Floor, CAPE TOWN Tel: (021) 466 7160 Fax 021 432 2830

[www.labour.gov.za](http://www.labour.gov.za)

**NATIONAL ASSEMBLY**

**WRITTEN REPLY**

**QUESTION NUMBER: 1499 [NW1706E]**

**1499.** **Mr S L Ngcobo (IFP) to ask the Minister of Employment and Labour:**

What are the initiatives and interventions of his department in collaboration with other sister departments, non-government organisations, agencies and institutions aimed at providing cyber-security learning to address the global deficit in the cyber-security workforce? NW1706E

**REPLY:**

Most of the Departments, if not all, Department of Employment and Labour included are governed by Department of Public Service and Administration (DPSA) ICT Governance Policy Framework which guides on overall ICT Governance and Information Security processes that we should follow and implement as the government entity.

There is a committee at DPSA that deals will cyber security related matters called “Standing Committee on Information Systems Security (SCISS)”, as the department, we are standing member of that committee and this is where all other government departments are represented to discuss matters related to information security and cyber-security.

The SCISS has come up with an initiative of departments sharing resources and transferring skills to one another in matters relating to cybersecurity. The initiative is still at the beginning stage where a database of cybersecurity specialists in the public sector is being developed.

Internal Information Security staff have also subscribed with other global threat security intelligent institutions i.e. Microsoft- Security Slate, Centre for internet Security (CSI) and Hackers Choice, where we regularly receive ICT security related awareness’s, newsletters, information on vulnerabilities, viruses and data privacy related breaches that the department should be aware of.