|  |
| --- |
| MEMORANDUM FROM THE PARLIAMENTARY OFFICE |

**NATIONAL ASSEMBLY**

**FOR WRITTEN REPLY**

**QUESTION 1506**

**DATE OF PUBLICATION OF INTERNAL QUESTION PAPER: 21/05/2021**

**INTERNAL QUESTION PAPER NO 14 OF 2021**

**Mr M N Nxumalo (IFP) to ask the Minister of Higher Education, Science and Innovation:**

Whether, in light of the upcoming Jobs Reset Summit of the World Economic Forum which will be held on 1-2 June and focus on mobilising a global jobs recovery plan in the wake of the COVID-19 global pandemic including the choices made by policy-makers, business leaders, workers and learners today which will shape societies for years to come and a focus on the closing of the cybersecurity skills gap that could help to create jobs and ensure businesses are safe, his department has (a) plans in place and (b) initiatives to provide cybersecurity learning to address the global deficit in the cybersecurity workforce; if not, why not; if so, what are the relevant details?

**NW1713E**

**REPLY:**

**DEPARTMENT OF SCIENCE AND INNOVATION**

I thank the Honourable Mr. Nxumalo for highlighting the importance of cybersecurity in an increasingly digital world. In terms of cybersecurity skills, the focus of the Department of Science and Innovation (DSI) is on research and development and high-level skills. With respect to R&D and skills, the DSI has, over the last 10 years, implemented a few programmes contributing to high-level human capital development, the development of innovative Information Security products for improved service delivery and self-reliance, and the provision of state-of-the-art RD-enabling infrastructure.

With respect to high-level human capital development, the DSI funded an intervention at the CSIR to develop a critical mass of skills in Information Security competency. The programme was targeted at MSc and PhD level. In order to grow the pool of women practitioners in the Information Security field, there was deliberate focus on recruiting and supporting young, Black female undergraduate students.

Through a High-end infrastructure grant, the DSI also funded the Network Simulation and Emulation Laboratory (NSEL) at the CSIR. This facility/ platform is used by the CSIR to provide training in various aspects of cybersecurity. Besides university students, the platform was also used to deliver training to governments agencies such as the Defence Intelligence and interns.

Research, development and innovation projects that contributed to service delivery and self-reliance include:-

* An optical coherence tomography (OCT)-based contactless fingerprint acquisition device (FPAD) and investigated the feasibility of the technology for lifting latent fingerprints for forensics. The results of the latent fingerprint investigation have indicated that it is possible to use this technology for fingerprint forensics. This is the course the CSIR is pursuing currently.
* The development of a prototype for biometric recognition system for minors.

Moving forward, cybersecurity has been identified as a key foundational digital technology in the decadal plan on science, technology and innovation. More detailed implementation planning is underway to put in place a more ambitious R&D and high-level skills development programme for the next 10 years. This programme will include R&D in blockchain-based solutions that are beyond cryptocurrencies with the related science and innovation instruments being geared towards their enablement.

It is anticipated that these solutions will be implemented within the emerging national cybersecurity framework in both the public and private sectors.

**DEPARTMENT OF HIGHER EDUCATION AND TRAINING**

|  |  |  |  |
| --- | --- | --- | --- |
| **Media, Information and Communication Technologies Sector Education and Training Authority (MICT SETA)** | | | |
| **(a) Plans in place** | **(b) Initiatives to provide cybersecurity learning to address the global deficit in the cybersecurity workforce** | **If not, why not** | **If so, what are the relevant details?** |
| To develop an Occupational Certificate: Cyber Security Analyst  To implement the programme for unemployed, retrenched and those in the workforce | The qualifications have been developed and submitted to QCTO for verification and submission to SAQA. |  | The qualification will cover the following components:  Knowledge module NQF Level 4  Practical skills module NQF Level 5  Work experience module NQF Level 5  Once approved the qualification will be implemented for a period of 12 months. |
| To develop a skills programme in Cyber Security | The process of development is underway |  | Once approved the skills programme will be implemented for two weeks. |
| To raise cyber security awareness within MICT SETA | MICT SETA will continue to raise cyber security awareness through campaigns and training to its personnel. |  | Some of the plans and initiatives which were started and will continue to be practised include:   * Cyber security awareness talks/sessions hosted by the Chief Information Officer, and Marketing and Communications Directorate inviting an external stakeholder to educate and create awareness on cyber security to MICT SETA personnel. * Cyber security awareness communication to all MICT SETA personnel through email systems. * Training of ICT personnel on cyber security. |
| Cyber Security Learning Programme | In progress. |  | MICT SETA is currently funding the Cyber Security Short Programme for 43 learners. |
| Cyber Security Learning Programme | In progress. |  | MICT SETA is currently funding the Cyber Security Graduate Internship Programme for 10 Interns. |