NATIONAL ASSEMBLY

QUESTION FOR WRITTEN REPLY

PARLIAMENTARY QUESTION NO: 2537

DATE OF QUESTION: 19 NOVEMBER 2021

DATE OF SUBMISSION: 03 DECEMBER 2021

Adv G Breytenbach (DA) to ask the Minister of Justice and Correctional Services:

(1) Whether, with reference to the recent ransomware attack on his department's Information and Communication Technology (ICT) systems, the information that became encrypted after being targeted has been decrypted; if not, why not; if so; what are the relevant details;

(2) whether (a) the targeted information is now available to his department in its entirety and (b) his department's ICT system is fully restored and productive at full capacity; if not, why not, in each case; if so; what are the relevant details in each case;

(3) whether his department has been able to determine exactly what information was targeted; if not, what is the position in this regard; if so, what (a) percentage of information has been compromised and (b) has become of the compromised information;

(4) whether the affected persons have been informed that their personal information may have been compromised; if not, why not; if so; what are the relevant details;

(5) whether his department has (a) been able to identify the ransomware attackers and (b)(i) received a ransom demand and (ii) paid ransom to the ransomware attacker(s); if not, what is the position in each case; if so, what steps is his department taking in each case?

NW2960E

REPLY:

1) The information or data that was encrypted was never decrypted because it needs a special decryption key which the Department of Justice and Constitutional Development does not have. The ransomware attacker is the only one with the decryption key.

2) (a) The information that was encrypted is still there in an encryption format, there is no way of decrypting the information. The focus was never to decrypt the information, instead the information and systems was restored from the backup tapes.
   (b) The systems are fully restored and productive, but due to capacity constraints, the systems are not running at full capacity.

3) The Department is fully aware of the information that was targeted.
   (a) The Department is unable to quantify the targeted information in terms of percentages.
   (b) The Department cannot tell with certainty as to what happened to the compromised information.

4) The Department is not aware of any information that was exfiltrated, there's an ongoing forensic investigation by South African Police Services (SAPS), and hopefully the final SAPS report will help us to answer that question.

5) (a) So far, the Department is unable to identify the ransomware attackers and hopefully the SAPS forensic investigation report will reveal such information.
   (b) (i) No ransom demand letter was received by the Department.
   (ii) No ransom amount was paid to the attackers.