GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
**LOK SABHA**
**UNSTARRED QUESTION NO. 2820**
TO BE ANSWERED ON: 11.03.2020

## SMS BASED ONE TIME PASWORDS

**2820. SHRI L.S.TEJASVI SURYA:**

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether the Government uses Two-Factor Authentication for securing e-governance portals and services, and if so, the details thereof;

(b) whether the Government has taken cognisance of the ease with which Short Message Services (SMS) based One –Time Passwords or OTP can be intercepted by potential hackers due to its unencrypted nature, and if so, the details thereof and the reaction of the Government thereto; and

(c) whether the Government proposes to lead the international digital space and foster Digital India by completely replacing SMS based OTP with Time based One Time Passwords/TOTP or better available technologies, and if so, the details thereof?

## ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI SANJAY DHOTRE)

(a): Yes, Sir. Government has published in gazette notification on “e-Pramaan: Framework for e-Authentication”. It offers following multi-factor authentication:

- Password: Text Password and/or Image Password
- One Time Password(OTP): Mobile, e-Mail and/or Mobile App
- Digital certificate: DSC with Indian CA
- Biometrics: Fingerprint and IRIS (Currently Aadhaar based)

Service delivering eGovernance portals such as Goods and Services Tax (GST),Transportation services, Income-Tax, etc. are using two factor authentication.

(b): No incidence has come to the notice of Department of Telecommunication (DOT) where Short Message Services (SMS) based One Time Password (OTP) have been hacked. Short Message Services(SMS) does not travel on Transmission Control Protocol/Internet Protocol (TCP/IP) inside telecommunication networks but on the standard signalling channel in a secure manner.

(c): ePramaan framework provides Time Based One Time Password(TOTP) as a factor of electronics authentication and other alternative technologies for authentication are being explored.

********