1	2	3	4	5
2.	Shri Jitender Singh Bhatia	10.03.17	65,000/-	Consultant (Finance)
3.	Shri Man Singh Yadav	20.07.17	39320/- + (DA-DR)	Consultant (Enforcement)
4.	Shri Jeet Singh	02.06.16 (Relieved on 31.05.17)	29,000/-	Consultant (Hindi Translator)
5.	Shri Vijay Kumar Sharma	24.09.15 (relieved on 23.05.16)	20,000/-	Jr. Hindi Translator

Incidents of breach of Aadhaar data

1375. SHRI VINAY DINU TENDULKAR: Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) the number and details of incidents/cases where Aadhaar data was leaked/ breached;

(b) whether any investigation has been conducted against agencies which were responsible for the breach/leakage of Aadhaar data;

(c) if so, the details thereof along with the action taken against them;

(d) the extent to which the database of Aadhaar is secured along with the steps taken by Government to ensure the privacy/security of Aadhaar data; and

(e) the mechanism put in place for usage of Aadhaar data by Government agencies and the accountability of officials in case of negligence on their part in handling of such data?

THE MINISTER OF STATE IN THE MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI S. S. AHLUWALIA): (a) There have been no incidents/cases where Aadhaar data was leaked/ breached from Unique Identification Authority of India (UIDAI)'s Central Identities Data Repository (CIDR).

(b) and (c) Does not arise in view of (a) above.

(d) UIDAI data is fully secured/encrypted at all the times *i.e.* at rest, in transit and in storage. For, further strengthening of security and privacy of data, security

audits are conducted on regular basis and all possible steps are taken to make the data safe and protected. Strengthening of security of data is an ongoing process.

UIDAI's existing security controls and protocols are robust and capable of countering any attempts or malicious designs of data breach or hacking. Security of Aadhaar is of critical importance to the Government and has given it paramount significance. UIDAI constantly strengthens and reviews its infrastructure and ecosystems in line with the best International security practices and technological standards. UIDAI has multi-layered security and privacy considerations built into the core strategy of Aadhaar with three basic doctrines of minimal data, optimal ignorance and federated database which give higher level of security.

Various policies and procedures have been defined, which are regularly reviewed and updated thereby appropriately controlling and monitoring any movement of people, material and data in and out of secured and well-guarded UIDAI premises, particularly the data centers.

Legal status of UIDAI has further strengthened the security assurance of Aadhaar ecosystem manifold with enactment of The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 which has stringent penalties/ punishments for offenders. In the ibid Act, Chapter VI is on Protection of Information.

UIDAI is ISO 27001:2013 certified by STQC with respect to Information Security which has added another layer of information security assurance. Further in pursuance of sub-section (1) of Section 70 of the IT Act 2000, UIDAI data has also been declared as Protected System by National Critical Information Infrastructure Protection Centre.

(e) The usage of Aadhaar data by any agency is governed by The Aadhaar Act, 2016 and subsequent regulations framed thereunder which have adequate safeguards. Sharing of information with the authorised agencies is governed as per the provisions of the Aadhaar Act, 2016.

(i) Section 29 (1) of the Aadhaar Act, 2016 read together with Regulation 3(1) of the Aadhaar (Sharing of information) Regulations, 2016 categorically states that no core biometric information, collected or created under the Aadhaar Act, shall be shared with anyone for any reason whatsoever; or used for any purpose other than generation of Aadhaar numbers and authentication under the Act.

(ii) Regulation 4(1) of the Aadhaar (Sharing of information) Regulations,

2016 provides that core biometric information collected or captured by a requesting entity from Aadhaar number holder at the time of authentication shall not be shared for any reason whatsoever.

(iii) Regulation 4(2) of the Aadhaar (Sharing of information) Regulations, 2016 provides that identity information available with a requesting entity shall not be used for any purpose other than that specified to the Aadhaar number holder at the time of submitting identity information for authentication and shall not be disclosed further without the prior consent of the Aadhaar number holder.

(iv) Regulation (5) of the Aadhaar (Sharing of information) Regulations, 2016 ensures the responsibility of any agency or entity other than requesting entity with respect to Aadhaar number and subsequent Regulation (7) states that any contravention of the above-mentioned regulations shall constitute a violation of sub-section (2) of Section 29 of the Act.

(v) Section 30 of the Aadhaar Act, 2016 applies the rigours of the IT Act, 2000 and the rules thereunder whereby Biometric Information is deemed to be Sensitive personal information.

(vi) Additionally, Chapter VII of the Act lays down monetary penalties and imprisonment for unauthorized sharing of residents' identity information. Any violation to the provisions of The Aadhaar Act is a criminal offence.

Life-threatening online challenges on social media

1376. DR. BANDA PRAKASH: Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether Government is aware of dangerous, life-threatening online challenges spread through social media, *e.g.*, the Momo challenge, etc.;

(b) if so, the steps taken by Ministry to lessen their harm; and

(c) the preventive measures undertaken by the Ministry to curb these challenges?

THE MINISTER OF STATE IN THE MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI S. S. AHLUWALIA): (a) to (c) There had been media reports about alleged suicides/attempted suicides due to dangerous, life-threatening online challenges like Blue Whale Challenge game, Momo Challenge Game etc. Government has taken several steps and preventive measures to curb these challenges. These, *inter alia*, include:–