GOVERNMENT OF INDIA MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY LOK SABHA UNSTARRED QUESTION NO. 656 TO BE ANSWERED ON: 19.07.2017

JOB LOSSES IN IT SECTOR

656 : SHRIMATI SUPRIYA SULE: SHRI SATAV RAJEEV: SHRI RAM KUMAR SHARMA: SHRI DHANANJAY MAHADIK: SHRI P.R. SUNDARAM: DR. J. JAYAVARDHAN: ADV. JOICE GEORGE: SHRI MULLAPPALLY RAMACHANDRAN: SHRI MOHITE PATIL VIJAYSINH SHANKARRAO: DR. HEENA VIJAYKUMAR GAVIT:

Will the Minister of Electronics & Information Technology be pleased to state: -

- (a) whether the Government's attention has been drawn towards the slow digitisation and job losses in the IT sector, if so, the details of jobs being provided in IT Sector presently and the reasons for slow down in job growth in IT Sector;
- (b) whether the Government has assessed the number of people who have been rendered jobless in the IT Sector and if so, the details thereof;
- (c) whether the Government is planning to convene a meeting of bigwigs of the tech industry to get an outlook on the sector and the help that they need from the Government to expand India's digital economy and if so, the details thereof;
- (d) the other corrective steps taken by the Government to arrest job losses in the IT Sector;
- (e) whether the information technology sector has been providing employment to 40 lakh persons on an average annually; and
- (f) if so, the facts in this regard and the current status thereof?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI P. P. CHAUDHARY)

(a) and (b): According to National Association of Software and Services Companies (NASSCOM), the IT-ITeS industry is estimated to employ nearly 39 lakh people in 2017, an addition of ~170,000 people over FY 2016. There is a continuing trend of gentle deceleration in net hiring growth rate (but with a growing base) as industry focuses on innovation, new digital technologies and enhanced efficiencies. Companies are re-aligning and re-adjusting themselves to the changing business scenarios and adjusting their workforce accordingly. Additionally, technologies such as advanced robotics and automation are changing job roles drastically across industries.

(c) and (d): Ministry of Electronics and Information Technology has already conducted a high level round table discussion on 16-06-2017 with bigwigs of the IT-ITeS industry for developing the roadmap for one trillion dollar digital economy of India.

(e) and (f): According to NASSCOM, employment to 40 lakh persons on an average annually by the IT industry is not tracked. However, the industry is estimated to employ nearly 39 lakh people currently, an addition of ~170,000 people over FY 2016. The trend over the last 3 years is as follows:

Year	Number of Total employees	Net addition during the year	Growth in Total employees
FY2014-15	3,485,000	217,000	7%
FY2015-16	3,688,000	203,000	6%
FY2016-17	3,863,000	175,000	5%

GOVERNMENT OF INDIA MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY LOK SABHA UNSTARRED QUESTION NO.612 TO BE ANSWERED ON 19.07.2017

SEMI -CONDUCTOR MANUFACTURING UNIT

612: SHRIMATI JAYSHREEBEN PATEL:

Will the Minister of Electronics & Information Technology be pleased to state:

- (a) whether the Government is considering to set up second fabrication facility in Gujarat, where conducive policy environment, development in the field of semi-conductors manufacturing and leading edge of Gujarat in manufacturing exists, which makes it a very good case for manufacturing Analog Integrated Circuits/ Solar PV cells and wafers;
- (b) if so, the details thereof; and
- (c) if not, the reasons therefor?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI P. P. CHOUDHARY)

(a), (b) and (c): Ministry of Electronics and Information Technology has issued a Letter of Intent dated 19.03.2014 to M/s. HSMC Technologies India Pvt. Ltd. (with ST Microelectronics and Silterra Malaysia Sdn. Bhd. as partners) for setting up Semiconductor Wafer Fabrication (FAB) facility with proposed location at Prantij, Gujarat. Also, under Modified Special Incentive Package Scheme (M-SIPS), two proposals for setting up vertically integrated Solar Photovoltaic (PV) facilities at Kutch, Gujarat have been submitted by M/s. Mundra Solar Photovoltaic Ltd.

GOVERNMENT OF INDIA MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY LOK SABHA UNSTARRED QUESTION NO. 469 TO BE ANSWERED ON: 19.07.2017

CYBER SECURITY

469 SHRI SISIR KUMAR ADHIKARI:

Will the Minister of Electronics & Information Technology be pleased to state:-

- (a) whether India ranks 4th globally in cyber threats of hacking data;
- (b) if so, the action proposed by the Government on security breaches therefor;
- (c) whether India has an instance of increase in cyber fraud from 3.4 per cent in 2015 to 5.1 per cent in 2016 therein; and
- (d) if so, the proposed action of the Government to prevent such attacks/threats?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI P.P. CHAUDHARY)

(a): There have been some media reports based on the survey by Symantec indicating India ranks 4th globally in cyber threats of hacking data.

(c): With the proliferation of Information Technology and related services there is a rise in instances of cyber crimes in the country like elsewhere in the world. As per the data maintained by National Crime Records Bureau (NCRB), a total of 9622 and 11592 cyber crime cases were registered during the years 2014 and 2015 respectively, showing a rise of 20% during 2014 to 2015. This includes cases registered under the Information Technology (IT) Act, 2000 and related sections of Indian Penal Code and Special & Local Laws involving computer as medium/ target. Similar data for the year 2016 is under collection. Further, as per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total no. of 44679, 49455, 50362 and 27482 cyber security incidents were observed during the year 2014, 2015, 2016 and 2017 (till June) respectively. The types of cyber security incidents include phishing, scanning/probing, website intrusions and defacements, virus/malicious code, ransomware, Denial of Service attacks, etc.

(b) and (d): Government has taken a number of legal, technical and administrative policy measures for addressing cyber security. These include the following, namely:-

- I. Enactment of the Information Technology (IT) Act, 2000 which has adequate provisions for safety of sensitive personal information.
- II. Government is implementing a Framework for enhancing cyber security, with a multi-layered approach for ensuring defence-in-depth and clear demarcation of responsibilities among the stakeholder organizations in the country.
- III. Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) as per the provisions of Section 70A of the IT Act, 2000 for protection of Critical Information Infrastructure in the country.
- IV. The CERT-In, a statutory authority under IT Act, 2000, issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has published guidelines for securing IT infrastructure, which are available on its website (www.certin.org.in). In order to detect variety of threats and imminent cyber attacks from outside the country, periodic scanning of cyber space is carried out.
- V. Government has initiated setting up of National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.

- VI. Cyber Crime Cells have been set up in all States and Union Territories for reporting and investigation of Cyber Crime cases.
- VII. Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of law enforcement personnel and Judiciary in these States.
- VIII. Industry associations such as Data Security Council of India (DSCI), NASSCOM, Cyber Forensic Labs, set up in certain States, have taken up tasks of awareness creation and training programmes on Cyber Crime investigation. Academia like National Law School, Bangalore and NALSAR University of Law, Hyderabad are also engaged in conducting several awareness and training programmes on Cyber Laws and Cyber crimes for judicial officers.
 - IX. A number of Cyber forensics tools for collection, analysis and presentation of the digital evidence have been developed indigenously and such tools are being used by law enforcement Agencies.
 - X. CERT-In and Centre for Development of Advanced Computing (C-DAC) are involved in providing basic and advanced training to law enforcement agencies, Forensic labs and judiciary on the procedures and methodology of collecting, analysing and presenting digital evidence.
 - XI. Reserve Bank of India (RBI) issues Circulars/advisories to all Commercial Banks on phishing attacks and preventive / detective measures to tackle phishing attacks. RBI also issues advisories relating to fictitious offers of funds transfer, remittance towards participation in lottery, money circulation schemes and other fictitious offers of cheap funds.
- XII. All banks have been mandated to report cyber security incidents to CERT-In expeditiously.
- XIII. All authorised entities/banks issuing Prepaid Payment Instruments (PPIs) in the country have been advised to carry out audit by the empanelled auditors of CERT-In on a priority basis and take immediate steps thereafter to comply with the findings of the audit report and ensure implementation of security best practices. Government has empanelled 54 security auditing organisations to support and audit implementation of Information Security Best Practices.
- XIV. Government has formulated Cyber Crisis Management Plan for countering cyber attacks for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors. Regular workshops are conducted for Ministries, Departments, States & UTs and critical organizations to sensitize them about the cyber security threat landscape and enabling them to prepare and implement the Cyber Crisis Management Plan.
- XV. Government has launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same for banks as well as common users.
- XVI. Ministry of Home Affairs has issued National Information Security Policy and Guidelines (NISPG) to Government organizations to ensure safety of data and minimize cyber threats.
- XVII. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 15 such drills have so far been conducted by CERT-In where 148 organisations from different states and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc have participated.
- XVIII. CERT-In is conducting cyber security trainings for IT / cyber security professionals including Chief Information Security Officers (CISOs) of Government and critical sector organisations. 14 training programs covering 431 participants and 13 training programs covering 329 participants were conducted during 2016 and 2017 (till June).
 - XIX. Ministry of Electronics & Information Technology (MEITY) regularly conducts programs to generate information security awareness. Specific book, videos and online materials are developed for children, parents and general users about information security which are disseminated through Portals like "http://infosecawareness.in/" and "www.cyberswachhtakendra.in"

GOVERNMENT OF INDIA MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY LOK SABHA UNSTARRED QUESTION NO. 504 TO BE ANSWERED ON: 19.07.2017

CERT-IN

504 SHRI V. ELUMALAI:

Will the Minister of Electronics & Information Technology be pleased to state:-

- (a) whether the Government has asked all digital payment agencies to report to CERT-In (Computer Emergency Response Team) regarding any unusual activity that they see on their platforms and if so, the details thereof;
- (b) whether the Government is undertaking a massive programme to create awareness among administrators, judges etc. and if so, the details thereof;
- (c) whether to strengthen cyber security, the Government has approved various new posts in CERT-In and State CERTs; and
- (d) if so, the details thereof?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI P.P. CHAUDHARY)

(a): All organisations providing digital payment services have been mandated to report cyber security incidents expeditiously to Indian Computer Emergency Response Team (CERT-In), a statutory body under IT Act, 2000.

- (b): Government is undertaking following initiatives to create awareness among administrators, judges etc. namely:-
- (i) Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of law enforcement personnel and Judiciary in these States.
- (ii) Industry associations such as Data Security Council of India (DSCI), NASSCOM, Cyber Forensic Labs, set up in certain States, have taken up tasks of awareness creation and training programmes on Cyber Crime investigation. Academia like National Law School, Bangalore and NALSAR University of Law, Hyderabad are also engaged in conducting several awareness and training programmes on Cyber Laws and Cyber crimes for judicial officers.
- (iii) Ministry of Electronics and Information Technology is implementing 'Information Security Education and Awareness (ISEA)' project to train professionals / government officials and create mass information security awareness among citizens. The Project is implemented by 52 institutions across the country. 20,369 persons had either been trained or were undergoing training in various formal/non-formal courses focusing on Cyber Security till 2016. Through direct training programs 3,718 Government personnel have been trained. So far, C-DAC Hyderabad has conducted 458 Awareness workshops for various user groups covering 51,225 participants from 24 States and 2 UTs including 7,559 participants from Central/State Government and police.
- (iv) CERT-In and Centre for Development of Advanced Computing (C-DAC) are involved in providing basic and advanced training to law enforcement agencies, Forensic labs and judiciary on the procedures and methodology of collecting, analysing and presenting digital evidence.
- (v) CERT-In is conducting cyber security trainings for IT / cyber security professionals including Chief Information Security Officers (CISOs) of Government and critical sector organisations. 18 such training programs were conducted covering 580 participants during the year 2016. In addition a workshop on security of digital payments systems has been conducted for stakeholder organisations covering 110 participants.

(c) and (d): To strengthen cyber security, during the period from April, 2014 to March, 2017, the following numbers of posts in CERT-In, Ministry of Electronics and Information Technology (MeitY) have been created/revived/ transferred with the approval of Ministry of Finance, Department of Expenditure, namely:-

- i. Department of expenditure vide I.D. No. 291642/E.Coord. 1 (2)/2016 dated 15.11.2016 has created 20 S&T posts for Cyber Swachhta Kendra, a project under CERT-In.
- ii. Department of Expenditure vide I.D. No. 312896/E.Coord.I/2016 dated 19.12.2016 has created 65 S&T and Non-S&T posts for National Cyber Coordination Centre under CERT-In.
- iii. 26 numbers of S&T and Non-S&T posts for CERT-In have been revived in 2016.
- iv. 8 numbers of S&T posts for CERT-In have been revived in 2016.
- v. Beside above 22 S&T posts have been/being transferred by MeitY to CERT-In in phased manner. These were created for CERT-In activities in the year 2006 while CERT-In was a project of the then Department of Electronics and Information Technology.

GOVERNMENT OF INDIA MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY LOK SABHA UNSTARRED QUESTION NO. 518 TO BE ANSWERED ON: 19.07.2017

CYBER SECURITY FOR GSTN

518 SHRIMATI RAKSHATAI KHADSE:

Will the Minister of Electronics & Information Technology be pleased to state:-

(a) whether Government proposes to set up a separate cyber security entity for GSTN (Goods Tax Network); and

(b) if so, the details thereof and the progress made so far in this regard?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI P.P. CHAUDHARY)

(a): There is no proposal to set up a separate Cyber Security Entity for GSTN. The cyber security is part of GST system and a dedicated Security Operations Command Center (SOOC) is operational 24x7x365 as part of GSTN.

(b): Does not arise.

GOVERNMENT OF INDIA MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY LOK SABHA UNSTARRED QUESTION NO. 588 TO BE ANSWERED ON: 19.07.2017

CYBER ATTACK

588 SHRI JITENDRA CHAUDHURY: SHRI DHARAM VIRA: SHRI HARISH MEENA: SHRI KUNWAR PUSHPENDRA SINGH CHANDEL: SHRI RAJU SHETTY: SHRI R. DHRUVA NARAYANA:

Will the Minister of Electronics & Information Technology be pleased to state:-

- (a) whether recently there was a world-wide cyber attack including India;
- (b) if so, the details thereof and the damages caused as a result thereof;
- (c) the steps being taken by the Government in this regard;
- (d) whether any study has been conducted to identify the cyber threats in the country and if so, the details thereof;
- (e) whether adequate number of cyber security experts are available in the country and if so, the steps being taken in this regard; and
- (f) whether Government is planning to amend the existing regulations for promotion of cyber security and if so, the steps being taken in this regard, so far?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI P.P. CHAUDHARY)

(a) and (b): Propagation of ransomware called WannaCry / WannaCrypt has been reported in many countries around the world including India since 12 May 2017. Propagation of another ransomware called Petya was also reported since 27 June 2017. Ransomware is a type of malicious software that infects a computer and restricts users' access to affected files by encrypting them until a ransom is paid to unlock it.

34 incidents have been reported to the Indian Computer Emergency Response Team (CERT-In) from organisations and individuals regarding infections of Wannacry and Petya ransomware. As reported to CERT-In, operations of one sea port were partially affected by the Petya ransomware. Remedial measures to contain damage and prevent such incidents have been advised by CERT-In.

(c): The following steps have been taken by the Government to prevent recent ransomware attacks, namely:-

- i. CERT-In has issued an advisory regarding detection and prevention of Wannacry ransomware on its website on 13 May 2017. Advisory regarding detection and prevention of Petya ransomware was issued by CERT-In on 27 June 2017.
- ii. CERT-In has issued a vulnerability note on its website with a Severity Rating of 'High' on March 15, 2017 suggesting information regarding vulnerabilities in Microsoft Windows systems which have been exploited by Wannacry ransomware alongwith remedial measures.
- iii. CERT-In has informed various key oragnisations in the country regarding the ransomware threat and advised measures to be taken to prevent the same. A webcast was also conducted in this regard for organisations and users.
- iv. Free tools for detection and removal of wannacry ransomware have been provided on the website of Cyber Swachhta Kendra (www.cyberswachhtakendra.gov.in).

Apart from the specific steps mentioned above, the following steps have also been taken to prevent malware/ransomware threats, namely:-

i. The CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect systems and mobile devices.

- ii. Government has launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same for banks as well as common users.
- iii. Security tips have been published for users to secure their Desktops and mobile/smart phones.
- iv. Ministry of Electronics & Information Technology (MEITY) regularly conducts programs to generate information security awareness. Specific book, videos and online materials are developed for children, parents and general users about information security which are disseminated through Portals like "http://infosecawareness.in/" and www.cyberswachhtakendra.in

(d): In tune with the dynamic nature of Information Technology and limited time available for an effective response, continuous efforts are required to be made to detect and prevent cyber attacks by way of continuous threat assessment and near real-time situational awareness. Such timely information enables coordinated actions by the stakeholders to take appropriate proactive and preventive actions.

Concerted efforts are being made to harvest the requisite information from multiple sources. These include incidents reported to and tracked by CERT-In, technical measures, security cooperation arrangement with overseas Computer Emergency Response Teams (CERTs) and leading security product and service vendors as well as agencies within the government. In addition, the study reports published by various agencies across the world are also studied to understand the historical data with respect to global threat landscape and threat predictions. As such, Government has not conducted a separate study to identify cyber threats.

(e): Towards enhancing qualified cyber security manpower, following steps have been taken, namely:-

- i. Ministry of Electronics and Information Technology is implementing the Information Security Education and Awareness (ISEA) project which aims to generate 1.14 lakhs qualified professionals at various levels in period of 5 years. A total of 52 institutions in various categories across the country are participating in the project. Besides, National Institute of Electronics and Information Technology (NIELIT) is conducting certification courses for creation of cyber security professionals.
- ii. CERT-In conducts regular training programme to make the network and system administrators aware about securing the IT infrastructure and mitigating cyber attacks. CERT-In is regularly conducting Cyber Crisis Management Plan (CCMP) workshops for Central Government Ministries/Departments, States & UTs and critical sector organisations to sensitise them about the cyber security threat landscape, enabling them to prepare and implement the Cyber Crisis Management Plan as well as participate in the mock drill exercises.
- iii. Cyber forensics training lab has been set up at Training Academy of Central Bureau of Investigation (CBI), Ghaziabad to impart basic and advanced training in cyber forensics and investigation of cybercrimes to police officers. In addition, Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of law enforcement personnel and Judiciary in these States.
- iv. Data Security Council of India (DSCI), NASSCOM and Cyber Forensic Labs set up in certain States, have taken up tasks of awareness creation and training programmes on Cyber Crime investigation. Academia like National Law School, Bangalore and NALSAR University of Law, Hyderabad are also engaged in conducting several awareness and training programmes on Cyber Laws and Cyber crimes for judicial officers.
- v. NASSCOM & DSCI have been working under the aegis of National Skill Development Corporation, Ministry of Skill Development and Entrepreneurship, on developing standardized content for the key job roles that have been identified based on the industry inputs, requirements and response.

(f):Presently there is no proposal with the Government to amend the Information Technology Act, 2000.

GOVERNMENT OF INDIA MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY LOK SABHA UNSTARRED QUESTION NO. 673 TO BE ANSWERED ON: 19.07.2017

LOSSES DUE TO CYBER ATTACK

673 SHRI JYOTIRADITYA M. SCINDIA: SHRI KAMAL NATH:

Will the Minister of Electronics & Information Technology be pleased to state:-

- (a) whether the Union Government is aware that many Indian companies are losing several crores every year due to cyber attacks;
- (b) if so, whether the Union Government in consultation with State Governments propose to strengthen the cyber attack laws;
- (c) if so, the details thereof;
- (d) whether any separate wing has been created to check such cyber attacks and to prosecute the culprits involved; and
- (e) if so, the details thereof?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI P.P. CHAUDHARY)

(a): The field of Information Technology (IT) is characterized by rapid developments and fast changing obsolescence. With every IT product introduced into the market, newer vulnerabilities are discovered, leaving scope for malicious actions. In tune with the dynamic nature of Information Technology, continuous efforts are required to be made to prevent and recover from cyber attacks. Malicious users continuously target India's IT infrastructure to infiltrate and hamper the functionality of IT systems. As such, the protection of India's IT infrastructure in general and critical information infrastructure in particular is a dynamic activity and continuing process. As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total no. of 44679, 49455, 50362 and 27482 cyber security incidents were observed during the year 2014, 2015, 2016 and 2017 (till June) respectively. The types of cyber security incidents include phishing, scanning/probing, website intrusions and defacements, virus/malicious code, ransomware, Denial of Service attacks, etc. No separate data with regard to the losses incurred by the Indian companies as a result of cyber attacks is maintained by Indian Computer Emergency Response Team (CERT-In) or Ministry of Corporate Affairs.

(b) and (c): The Information Technology Act, 2000, as amended from time to time, provides legal framework to deal with the cyber security breaches.

(d) and (e): The Indian Computer Emergency Response Team (CERT-In) has been designated as the nodal agency for responding to cyber security incidents in the country as per provisions of Section 70B of the Information Technology Act, 2000 as amended from time to time. National Critical Information Infrastructure Protection Centre (NCIIPC) has been created as per provision of Section 70A of the Information Technology Act, 2000 to act as the nodal agency for protection of critical information infrastructure. Information Technology Act 2000 provides for punishment for various cyber crimes. CERT-In is operating a round the clock incident response held desk, issuing alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures, conducting training programs on specific areas of cyber security and conducting mock drills to enable assessment of cyber security posture and preparedness of organizations.

GOVERNMENT OF INDIA MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY LOK SABHA UNSTARRED QUESTION No. 485 TO BE ANSWERED ON: 19.07.2017

DIGIGAON PROJECT

485. SHRIMATI V. SATHYA BAMA:

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

- (a) whether Government has envisaged DigiGaon, a pilot project of Digital villages to be implemented in 1050 Gram Panchayats in the country;
- (b) if so, the State-wise list of Gram Panchayats selected/to be selected under DigiGaon project and the amount allocated/sanctioned for each Gram Panchayat;
- (c) whether the Government has any idea/plans to involve IT companies/NGO's to create more Digital villages in the country; and
- (d) if so, the details thereof?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI P. P. CHAUDHARY)

(a): Yes, Madam. The Government has approved a Pilot Project called 'DigiGaon'.

(b): The DigiGaon project has been approved to be implemented in 1050 Gram Panchayats (GPs) spread across 30 States/UTs. However, after assessment of the readiness of the States/UTs, and recommendations of the Empowered Group of DigiGaon, the project will be piloted in three States out of the following five states, viz. Bihar, Chhattisgarh, Gujarat, Madhya Pradesh and Uttar Pradesh. The 'DigiGaon project envisages providing telemedicine, tele-education, LED lighting, Wi-Fi hotspots and skill development in the selected Gram Panchayats (GPs) and does not entail any GP wise budgeting allocation/sanction of funds.

(c) and (d): No, Madam.

GOVERNMENT OF INDIA MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY LOK SABHA UNSTARRED QUESTION NO. 528 TO BE ANSWERED ON: 19.07.2017

PURPOSE OF AADHAAR DATA

528. SHRI M.K. RAGHAVAN:

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

- (a) whether the data collection under Aadhaar is only to ensure that welfare and pension scheme funds and public distribution system reach the poor or is it invasion of privacy;
- (b) if so, whether such collection is infringing upon the citizens fundamental rights;
- (c) if so, the areas where Aadhaar card has been made compulsory for an individual;
- (d) whether Aadhaar is now primarily required for income tax returns and if so, the details thereof;
- (e) whether the creation of PAN card for the purpose of income tax has failed to serve the purpose and is necessitating Aadhaar linkage; and
- (f) if so, the areas which were found harmful under PAN scheme and the steps taken to overcome these loopholes in detail?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI P.P. CHAUDHARY)

(a) and (b): The role of UIDAI, under the Ministry, is to issue Aadhaar numbers and provide authentication services for establishing identity of the beneficiaries. Accordingly, as per Section 3 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act, 2016"), every resident is entitled to obtain an Aadhaar number.

The usage of Aadhaar for delivery of welfare service benefits or any other purpose and the extent to which Aadhaar is to be used is to be determined by the implementing agencies such as State Governments/Central Ministries and other agencies.

The usage of Aadhaar is governed by the Aadhaar Act, 2016. Section 7 of the Act provides that the Central Government, or as the case may be, the State Government, may for the purpose of establishing identity of an individual as a condition for receipt of a subsidy, benefit or service for which expenditure is incurred from the Consolidated Fund of India, require that such individual undergo authentication, or furnish proof of possession of Aadhaar number or in the case of an individual to whom no Aadhaar number has been assigned, such individual shall make an application for enrolment. Section 7 further provides that, if an Aadhaar number is not assigned to an individual, the individual shall be offered alternate and viable means of identification for delivery of the subsidy, benefit or service.

Further, provisions of Section 57 of the Aadhaar Act inter alia permit the usage of Aadhaar number for establishing the identity of an individual for any purpose pursuant to any law or any contract to this effect with the requirement of being compliant of the provisions of Section 8 and Chapter VI of the Aadhaar Act. There is no infringement upon the citizens' fundamental rights.

The Aadhaar Act, 2016 is all encompassing legislation addressing issues of data protection and confidentiality of the UIDAI database. The Aadhaar (Data Security) Regulations & Aadhaar (Sharing of Information) Regulations, 2016 augment the measures for ensuring privacy and data protection.

(c): As on 13.07.2017, 123 schemes of various Central Ministries/ Departments have been notified under Section 7 or 57 of Aadhaar Act, 2016. In respect of these schemes, Aadhaar number is necessary for the purpose of establishing identity of an individual to enable receipt of subsidies, benefits and services etc .

(d): Section 139AA of the Income Tax Act, 1961, introduced by the Finance Act, 2017, has a provision that every person who is eligible to obtain Aadhaar number shall, on or after the 1st day of July, 2017, quote Aadhaar number or Enrolment ID of Aadhaar application form in the return of income. Vide notification number 37/2017, bearing S.O.1513(E), it has been notified that the provisions of section 139AA of the IT Act, 1961 shall not apply to an individual who does not possess the Aadhaar number or the Enrolment ID and is:

- (i) residing in the States of Assam, Jammu and Kashmir and Meghalaya;
- (ii) a non-resident as per the Income Tax Act, 1961;
- (iii) of the age of eighty years or more at any time during the previous year; or,
- (iv) not a citizen of India.

(e) and (f): PAN is the key identifier of taxable entity and aggregator of all financial transactions undertaken by the entity. One PAN for one person is the guiding principle for allotment of PAN. However, for achieving the objective of one PAN to one assessee, it is required to maintain uniqueness of PAN.

The uniqueness of PAN is achieved by conducting a de-duplication check on all already allotted PAN against the data furnished by new applicant. Under the existing system of PAN, only demographic data is captured. Some instances were found where multiple PANs have been allotted to one person or one PAN has been allotted to multiple persons despite the application of de-duplication process based on demographic data. Linkage of Aadhaar number into PAN database will allow a robust way of de-duplication as Aadhaar number is based on biometric attributes of finger prints and iris images. Further, seeding of Aadhaar will allow weeding out any undetected duplicate PANs.

GOVERNMENT OF INDIA MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY LOK SABHA UNSTARRED QUESTION NO. 574 TO BE ANSWERED ON: 19.07.2017

LEAKAGE OF AADHAAR DATA

574. SHRI M.B. RAJESH:

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

(a) whether the Government has taken note of leakage of Aadhaar data from various Government Departments;

(b) if so, the number of instances of Aadhaar data leakages noticed from various Government departments and agencies;

(c) whether private players have acquired Aadhaar data including biometric details of customers; and

(d) if so, the details thereof and the steps taken by the Government in this regard?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI P.P. CHAUDHARY)

(a) and (b): There has been no leakage of Aadhaar data from UIDAI. However, it was found that around 210 websites of Central Government, State Government Departments including educational institutes were displaying the list of beneficiaries along with their name, address, other details and Aadhaar numbers for information of general public. UIDAI has taken note of the same and is regularly monitoring the status to get the Aadhaar data removed from the said websites.

(c) and (d): Private players have not acquired any Aadhaar Data including biometrics from UIDAI. The sharing of Aadhaar information is done only with authorized KYC User Agencies (KUAs)/ Authentication User Agencies (AUAs) (both can be Government or private agencies), through authorized secure applications after following well established security procedures and protocols. The sharing of Aadhaar information is regulated in terms of the Aadhaar (Sharing of Information) Regulations, 2016, framed under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

GOVERNMENT OF INDIA MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY LOK SABHA UNSTARRED QUESTION NO. 514 TO BE ANSWERED ON: 19.07.2017

CELL PHONE QUALITY

514. SHRIMATI KOTHAPALLI GEETHA:

Will the Minister of Electronics and Information Technology be pleased to state: -

- (a) whether the Government has any system in place to check the quality of cell phones quality to avoid call drops and to ensure data speed and if so, the details thereof and if not, the reasons therefor;
- (b) whether many unlicensed companies and untested companies without valid certificates are manufacturing thousands and lakhs of smart phones and selling in the market throwing safety measures in the air and if so, the details thereof and reasons therefor;
- (c) whether LTE smart phones with the facility of having 2 sims are not maintaining data speed properly and there is need to adopt a policy decision by the Government in this regard and if so, the details thereof and the steps being taken in this regard; and
- (d) whether the consumers are facing lot of difficulties after purchasing such smart phones in the market and if so, the details thereof and corrective steps being taken by the Government in this regard?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI P. P. CHAUDHARY)

(a): As per details provided by Indian Cellular Association (ICA), call drop rate and the other network parameters like Network Downtime: Percentage non-availability of mobile network in a month, percentage of calls made by subscribers and successful within operator's network, percentage of Calls with good voice quality call, etc. are monitored by Telecom Regulatory Authority of India (TRAI) on a regular basis. These parameters help determine the quality of network and benchmarking the performance. At present, internet data speed or mobile broadband speed offered to a subscriber is not measured or committed by the network operators to the subscriber. TRAI has recently flagged a consultation process on "Data Speed Under Wireless Broadband Plans" to help subscriber make an informed choice and choose suitable data plans. Owing to the various factors as pointed in the Consultation paper like variable number of concurrent users, distance of a user from the Base Transceiver station/NodeB/ eNodeB, peak time event or the type of application (video, text, etc.) being accessed, a minimal download speed for wireless/mobile networks is difficult to be committed by an operator. However, government can ensure a better subscriber experience by asking the operators to specify Minimum download speed in the network i.e. the worst performing speed as well as average download speed to clarify the network quality before releasing a mobile internet plan similar to ' US Broadband label' as suggested by TRAI in its consultation paper.

(b): Keeping in view the safety of Indian consumers, mobile phones have been notified under the "Electronics and Information Technology Goods (Requirements for Compulsory Registration) Order, 2012" for mandatory safety testing of the product as per IS 13252 (Part 1):2010 at Bureau of Indian Standards (BIS) recognized laboratories. The manufacturers have to get their product tested for safety compliance and seek registration from the BIS before selling in the market place. BIS has granted 948 registrations for mobile phones as on 13th July 2017.

(c) and (d): As per details provided by TRAI, 4G enabled dual SIM smart phones have issues relating to speed. In these phones only one slot is 4G enabled, which is either pre-defined by the manufacturer or which can be selected by the user through options in the phone. In general, there will be degradation in speed in case of these phones for specific scenario when both SIMs are being used at same time as the resources are shared for two SIMs. The extent of degradation may be dependent upon radio network type SIM configured by the customer and the type of services offered by the service provider such as 2G, 3G, 4G. In case 4G SIM is put in 3G/2G slot there will be relatively higher degradation and it may be reduced by putting SIM in appropriate slot. There could also be higher degradation in case two 4G SIMs are used by the customer and one of the service provider is offering only 4G services. As such, there is a need for educating the customers about the use of slots in the dual mobile handsets. The extent of degradation may also be reduced by improvements in algorithms provided by chip manufacturers. The mobile handset manufacturers are required to take appropriate action for improving algorithm used in this regard. TRAI had discussed the matter with the service providers, Industry Associations, Cellular Operators Association of India & Indian Cellular Association and chipset manufacturers. The Indian Cellular Association was advised to take up the matter with the manufacturers so as to upgrade the algorithm in the handsets. Also the service providers were advised to educate the consumers about proper use of SIM slot in dual SIM Smart Phones.

GOVERNMENT OF INDIA MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY LOK SABHA UNSTARRED QUESTION NO. 618 TO BE ANSWERED ON: 19.07.2017

IT IN RURAL AREAS

618 SHRI RAYAPATI SAMBASIVA RAO:

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

- (a) the major efforts taken in the last three years to take information technology to the rural areas of the country;
- (b) the details of funds that have been allocated to achieve this said target;
- (c) the percentage of rural areas covered by IT services;
- (d) the changes that have been brought about in the schemes under the Ministry in the last three years to take internet to the remote areas of the country; and
- (e) the details of rural areas of the country which have been penetrated by internet so far ?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI P. P. CHAUDHARY)

(a): Following are the major efforts made by Ministry of Electronics and Information Technology (MeitY) in the last three years to take information technology to the rural areas of the country:

(i) Common Services Centres (CSCs): CSCs are internet enabled centres operated by local entrepreneurs called Village Level Entrepreneurs (VLEs) and provide eServices to rural citizens. CSCs deliver various Government-to-Citizen (G2C) services, Business-to-Citizen (B2C) services, financial inclusion services, Educational services, Skill development services etc. to citizens.

The Ministry of Electronics and Information Technology (MeitY), Govt. of India is establishing CSCs in about 2.5 lakhs of Gram Panchayats (GPs) across the country (with at least one CSC in each GP). For this, MeitY approved a project- "CSC 2.0", in August, 2015 under Digital India Programme with an outlay of Rs. 475.11Crores which is to be implemented over a period of **four years**. M/s CSC e-Governance Services India Limited (a CSC Special Purpose Vehicle was engaged as the implementing agency for the project with active support and participation by the respective State/Union Territory (UT) Nodal Department(s), State Designated Agencies (SDAs), and, the District e-Governance Societies (DeGS).

Till **June**, **2017**, 3,00,774 Common Services Centres (CSCs) have been registered across the country, among which, 1,96,922 are at Gram Panchayat (GP) level. Out of the total registered CSCs, 2,61,071 CSCs are functioning and transacting for delivery of eServices, among which, 1,63,226 are at GP level.

Target CSCs at Gram Panchayat (GP) level	2,50,000 (approx.)		
	Registered	Functional	
CSCs at Gram Panchayat (GP) level (A)	1,96,922 (at 1,32,514 GPs)	1,63,226 (at 1,22,369 GPs)	
CSCs other than GP, including Urban (B)	1,03,852	97,845	
Total CSCs including GP (A+B)	3,00,774	2,61,071	

The State/UT-wise CSC roll out status is given in Annexure-I.

(ii) National Information Infrastructure (NII):

A pilot on National Information Infrastructure (NII) for a period of one year was initiated by MeitY in July, 2015 for one district each in the States of Nagaland, Karnataka, Kerala, Gujarat, Uttarakhand and UT of Chandigarh and Puducherry to integrate various ICT infrastructure namely State Data Centres (SDCs), State Wide Area Network (SWAN), National Knowledge Network (NKN), National Informatics Centre Network (NICNET), State Service Delivery Gateway (SSDG) including National Optical Fibre Network (NOFN)/BharatNet created in these States. The objective is to provide connectivity to government offices upto Gram Panchayat (GP) level (1059 GPs).

(b): Details of the funds that have been allocated to achieve this said target are indicated below:

<u>CSC 2.0</u>: Approved outlay = Rs. 475.11 crores, Released till date = Rs. 145 crores <u>National Information Infrastructure (NII)</u>: Approved outlay = Rs. 45.84 crores, Released till date = Rs. 45.84 crores

(c): Coverage of IT services in rural areas is detailed below:

(i) Through Common Services Centres (CSCs):

Various types of citizen centric eServices can be delivered through national level integrated platform of CSC-Digital Seva once State/UT level service access portals are integrated with Digital Seva portal. Number of services in national CSC portal (Digital Seva) was increased from 32 to 170 during last 3 years. Out of the total target of around 2.5 lakhs of Gram Panchayats (GPs) to be covered through CSCs under the ongoing CSC 2.0 project within 4 years (by August, 2019) for delivery of citizen centric eServices, more than 1.33 lakhs GPs (more than 53%) have been covered with around 1.97 lakhs of CSCs for delivery of eServices to citizens till June, 2017.

(d) and (e): Provisioning of internet connectivity at rural areas is under the purview of Department of Telecommunications (DoT), under Ministry of Communication.

DoT is implementing National Optical Fibre Network (NOFN) project, renamed as BharatNet. It is one of the pillars of Digital India Programme to establish network infrastructure by connecting all Gram Panchayats (GPs) (approx. 2.5 lakhs) in the country through Optical Fibre Cable (OFC) and by using an optimal mix of underground fibre, fibre over power lines, radio and satellite media, for providing broadband connectivity by all categories of service providers on non-discriminatory basis. The BharatNet project is planned to be implemented in three phases. Under first phase of the project, 1 lakh Gram Panchayats (GPs) is to be connected by laying underground OFC by November 2017. Under second phase, connectivity will be provided to remaining 1.5 lakhs GPs in the country using an optimal mix of underground fibre, fibre over power lines, radio and satellite media, by March, 2019. Under third phase, a state-of-the-art network with ring architecture, is planned to be completed by 2023.

Under the said project (phase-I), 2,38,489 KMs of pipeline has been laid in 1,06,276 GPs, 2.20 lakhs KMs of optical fibre pulled for 1,00,152 GPs and 23,147 GPs have been connected so far till 09-07-2017. The detailed status of BharatNet project is given in **Annexure-II**.

Apart from that, the CSC Special Purpose Vehicle (CSC -SPV) launched an initiative called- **Wi-Fi Choupal for 5,000 Gram Panchayat (GP)**, a rural Wi-Fi service initiative in financial year 2016-17 at the behest of Telecom Commission, Department of Telecommunications, Govt. of India at an estimated cost of Rs. 100 cr. Wi-Fi Choupal project has been launched to provide Wi-Fi Internet access in rural India through CSCs. As on date, Wi-Fi Infrastructure has been deployed in 2500 GPs across 9 States (Uttarakhand, Uttar Pradesh, Madhya Pradesh, Chhattisgarh, Haryana, Jharkhand, Bihar, Maharashtra, and Karnataka) and 2 Union Territories (Chandigarh and Puducherry). The activation of the internet service has been done at 650 GP locations.

<u>ANNEXURE – I</u>

	STATE/UT-WISE CSC ROLL OUT STATUS AS ON 30 JUNE, 2017						
S.	State	No. of Gram	No. of CSCs	No. of CSCs	No. of GPs	Total No. of	Total No. of
No.		Panchayat	Registered	Registered	covered	Functional	Functional
		(GP)	including	at GP level	with	CSCs	CSCs at GP
			GP		Registered CSC	including GP	level
		1	2	3	3.1	4	5
1	Andhra Pradesh	12833	5488	3475	3475	5212	3119
2	Arunachal Pradesh	1779	115	54	54	54	44
3	Assam	2196	2735	2246	2196	2213	1559
4	Bihar	8463	22380	17541	8463	19090	11960
5	Chhattisgarh	9734	11929	8410	8410	11175	7940
6	Goa	189	54	37	37	32	30
7	Gujarat	13735	18062	14845	13735	16805	13885
8	Haryana	6155	8724	5834	5834	7900	4923
9	Himachal Pradesh	3243	2624	2269	2269	2552	1952
10	Jammu & Kashmir	4128	2123	1039	1039	1727	900
11	Jharkhand	4423	9799	7445	4423	9014	5295
12	Karnataka	5628	6564	2665	2665	4963	2333
13	Kerala	979	2676	1969	979	2119	1111
14	Madhya Pradesh	23012	19446	13175	13175	16194	11873
15	Maharashtra	27920	31066	19464	19464	25324	17788
16	Manipur	165	646	256	165	554	207
17	Meghalaya	1463	262	193	193	198	74
18	Mizoram	776	376	316	316	316	176
19	Nagaland	1123	232	230	230	220	138
20	Odisha	6234	8651	6832	6234	6545	5599
21	Punjab	12800	6261	4282	4282	5229	3464
22	Rajasthan	9946	30436	15038	9946	29814	14878
23	Sikkim	165	37	31	31	31	23
24	Tamil Nadu	12618	11069	5773	5773	7408	4646
25	Telangana	8787	5564	3180	3180	5043	2855
26	Tripura	1038	521	442	442	366	322
27	Uttar Pradesh	51914	67054	41675	7555	58876	35804
28	Uttarakhand	7555	5594	4441	4441	4339	3853
29	West Bengal	3351	17527	13584	3351	15653	6330
	State Total	242352	298015	196741	132357	258966	163081
	Union Territory						
1	Andaman & Nicobar	69	49	26	26	42	20
2	Chandigarh	17	112	29	17	65	21
3	Dadra & Nagar	11	31	16	11	21	9
4	Daman and Dir	1 /	11	2	2	0	1
4	Daman and Diu	14	11	2	2	8 1954	1
3		0	2361	0	0	1854	0
0	Duduaharra	10	<u> </u>	<u> </u>	<u> </u>	2	2
/		98	192	105	98	2105	92
		219	2759	181	157	2105	145
	GRAND TOTAL	242571	300774	190922	152514	2010/1	103220

	STATUS OF BHARATNET AS ON 09.07.2017					
S.N.	Description of Work	Status				
1.	OFC Pipe laid	2,38,489 Kms (1,06,276 GPs)				
2.	Optical Fibre laid	2,20,139 Kms (100,152 GPs)				
3.	Tenders Finalized	3324 Blocks / 1,24,412 GPs				
4.	Work Started*	3223 Blocks / 1,20,570 GPs				
5.	Current Weekly performance of Optical Fibre laying	662Kms				
6.	Current Weekly performance of OFC Pipe laying	889 Kms				
7.	Optical Fibre Cable Delivered on site	2,55,499 Kms				
8.	GPON Integrated & Tested (Lit)	23,147 GPs				

* does not include the data of Andhra Pradesh

State-wise status of NOFN (BharatNet) as on 09.07.2017

S.N	States/ UTs	No. of Gram	Pipe laid	Cable laid	No. of GPs	No. of GPs GPs	
0.		Panchayats (GPs)- Phase I	(kms.)	(in kms)	where Pipe laid	where Cable laid	connected
1	Assam	1533	3799	4158	1420	1348	354
2	Bihar	5754	12199	12940	4967	4742	711
3	Chhattisgarh	4104	10213	7873	3304	3159	1289
4.	Harvana	6020	9776	10993	5907	5801	894
5.	Jammu & Kashmir	388	427	388	214	200	0
6.	Karnataka	6092	11784	12193	6026	6010	4826
7.	Kerala	977	720	830	1129	1129	1129
8.	Madhya Pradesh	12655	35904	31113	12026	11643	3599
9.	Maharashtra	15301	26696	25129	12664	11843	1992
10.	Punjab	8049	9810	9153	6989	6745	637
11.	Rajasthan	8194	21069	20268	7114	7046	1725
12.	Uttar Pradesh	27974	48556	44678	25363	23409	2785
13.	Uttarakhand	1863	2792	2636	1503	1463	431
14.	West Bengal	2637	5175	4876	1822	1791	231
15.	Andaman & Nicobar	69	0	0	0	0	0
16.	Chandigarh	12	18	19	12	12	12
17.	Arunachal Pradesh	863	1558	656	609	220	0
18.	Nagaland	994	2614	1475	831	462	0
19.	Manipur	904	333	232	154	122	26
20.	Mizoram	763	735	438	125	73	0
21.	Tripura	1021	1688	1584	834	810	79
22.	Meghalaya	1208	1212	525	433	191	0
23.	Gujarat	6905	10518	9542	5046	4478	1018
24.	Puducherry	98	82	92	98	98	101
25.	Andhra Pradesh	1673	2627	766	520	283	0
26.	Telangana	2017	4538	4462	2038	2038	206
27.	Odisha	3860	8121	7970	3109	3108	517
28.	Jharkhand	2713	5012	4669	1864	1775	529
29.	Himachal Pradesh	252	513	481	155	153	56
30.	Daman & Diu	15	0	0	0	0	0
31.	Dadra & Nagar Haveli	20	0	0	0	0	0
32.	Sikkim	52	0	0	0	0	0
33.	Lakshadweep	10	0	0	0	0	0
34.	Tamil Nadu	0	0	0	0	0	0
35.	Goa*	-	-	-	-	-	-
	Grand Total	124127	238489	220139	106276	100152	23147

*All the GPs of Goa are already connected with Optical Fibre

GOVERNMENT OF INDIA MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY LOK SABHA UNSTARRED QUESTION NO. 652 TO BE ANSWERED ON: 19.07.2017

CASHLESS ECONOMY

652. SHRI ANANTKUMAR HEGDE:

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

(a) whether the expansion of digital economy has taken place after the promotion of cashless economy in the country;

(b) if so, the assessment of the said expansion till date in year 2017 in comparison with the last year;

(c) whether it is a fact that a commission is charged on cash transactions under the digital economy; and

(d) if so, the percentage collected now on various mediums of transaction?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI P.P. CHAUDHARY)

(a) and (b): The total number of digital payment transactions over the period October, 2016 to May, 2017 is at Annexure I. The data indicates that there has been an increase in digital payments transactions during the said period.

(c) and (d): As per Reserve Bank of India (RBI) circular No. RBI/2014-15/72 dated 1st July 2014, scheduled commercial banks have freedom to levy charges for various services. An illustrative list of charges levied by some of the public sector banks on handling of cash is at Annexure-II.

<u>Annexure I</u>

#	Month	Total Digital Payment Transactions (In Crores)
1	Oct 2016	71.27
2	Nov 2016	83.48
3	Dec 2016	123.46
4	Jan 2017	114.96
5	Feb 2017	101.18
6	Mar 2017	119.07
7	April 2017	118.01
8	May 2017	111.45

Source: RBI and NPCI

Annexure-II

Bank	Charges on deposit and handling of cash in Savings Bank Accounts at bank branch (as on 7.7.2017)		
Allahabad Bank	No charges		
Andhra Bank	No charges		
	Home branch: No charges		
Bank of Baroda	Non-home branch: For cash deposit of up to Rs. $30,000$ per day per account, there is no charge. Thereafter, charge Rs.2.50 per thousand or part thereof, for amount in excess of Rs. $30,000$		
Bank of India	No charges		
Bank of Maharashtra	No charges		
Canara Bank	Free up to Rs. 50,000. Thereafter, a charge of Re. 1 per Rs. 1000, subject to a		
Canara Dalik	minimum of Rs. 50 and a maximum of Rs. 2,500/- per transaction		
Central Bank of Indla	No charges		
Corporation Bank	No charges		
Dena Bank	No charges		
IDBI Bank	In metro/urban locations, no charge up to 5 transactions per month. In semi- urban locations, no charge up to 7 transactions per month. In rural locations, no charge up to 10 transactions. Thereafter, a charge of Rs. 2.50 per Rs.1000 subject to a minimum of Rs. 25 and a maximum of Rs. 10,000 per month.		
	Non home branch: No charge for each deposit of up to Rs. 50000 per day		
Indian Bank	per account. Thereafter, charge of Po. 1 per thousand or part thereof		
	subject to a minimum of Rs. 25 for amount in excess of Rs 50,000		
Indian Overseas	No charges		
Bank Oriental Bank of	No cash deposit charges. No charge for cash handling on depositing up to Rs. 1 lakh per day, and above Rs 1 lakh per day, a charge of 10 paisa per piece (currency note)		
Punjab & Sind	No charges		
Bank	No charges at the home branch		
Punjab National Bank	For cash deposit at all branches within the same clearing centre and city (other than at the home branch) there are no charges up to Rs. 25,000 per day. Above Rs. 25000, charge of Re. 1 per Rs. 1000 or part thereof, with a minimum of Rs. 25 per transaction. For Cash Deposit at outstation non-home branches (other than in the same clearing centre/city), there are no charges up to Rs. 25,000 per day. Above Rs.		
	25,000, charge of Rs. 2 per Rs. 1000 or part thereof with a minimum of Rs. 25 per transaction		
State Bank of India	charges on transactions using Cash Deposit Machine (CDM).		
Syndicate Bank	No charges		
	No charges at the home branch Above Rs 50 000 per day at non-home branch a		
Union Don's of	charge of Re. 1/- per thousand, subject to a minimum of Rs. 10 and a		
Union Bank of	maximum Rs. 11.500		
United Bank of	No charges		
Vijaya Bank	No charges		

GOVERNMENT OF INDIA MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY LOK SABHA UNSTARRED QUESTION NO. 604 TO BE ANSWERED ON: 19.07.2017

WEBPAGE FOR GRIEVANCE REDRESSAL REGARDING GST

604. SHRI ANANDRAO ADSUL: SHRI DHARMENDRA YADAV: SHRI ADHALRAO PATIL SHIVAJIRAO: DR. SHRIKANT EKNATH SHINDE:

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

- (a) whether the Government is aware that there are various issues which are being faced by the companies to file grievance redressal with regard to GST implementation;
- (b) if so, the details thereof;
- (c) whether the Ministry has decided to launch a dedicated webpage for facilitating taxpayers with regard to addressing issues related to information technology services and electronic goods to ensure preparedness for GST implementation;
- (d) if so, the details thereof and the salient features therefor; and
- (e) the manner and extent to which it will be helpful for the general people and the companies/organisations in the implementation of GST?

ANSWER

MINISTER of STATE for ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI P. P. CHAUDHARY)

(a) and (b): No, Sir(s). There are no issues with regard to filing of grievance related to GST. The government is constantly monitoring the situation and is taking requisite action to address any issues that the trade might be facing in the implementation of GST. For this purpose, the government has created a dedicated website <u>https://cbec-gst.gov.in/feedback.html</u> to effectively handle any such issues.

(c) to (e): Ministry of Electronics and IT (MeitY) have created GST webpage (<u>www.meity.gov.in/GST</u>) on its' website to provide sector specific information and link to CBEC website on GST. The GST webpage of MeitY consists of four modules: (1) GST Grievance for ICT & E providing a form for filing GST Grievance/query for ICT & Electronics sector, (2) GST Rate for IT Services (Software), (3) GST Rate Schedule for Electronics sector, which provides information on the GST rate on software and electronics products, and, (4) GST Facilitation Cell which provides details of the chairperson and the sector specific members of the GST Facilitation Cell of MeitY. Queries/grievances received on MeitY website are acknowledged and further taken up by specific Groups/Organizations of MeitY for appropriate response.

Ministry of Electronics and Information Technology (Parliament Section)

Sl.	D.No.	Admit	Subject	File No.	Concd. GCs / HODs	Remarks
No.		No.				
1.	1016	469	Cyber Security	2(222)/17-Parl.	GC(AK)	
2.	1089	485	Digigaon Project	2(221)/17-Parl.	JS(RB)	
3.	1171	504	CERT-In	2(226)/17-Parl.	GC(AK)	
4.	1223	514	Cell Phone Quality	2(228)/17-Parl.	JS(SKR)	
5.	1261	518	Cyber security for GSTs	2(225)/17-Parl.	GC(AK)	
6.	1313	528	Purpose of Aadhaar data	2(211)/17-Parl.	JS(RB)	
7.	1430	574	Leakage of Aadhaar Data	2(214)/17-Parl.	JS(RB) / CEO, Aadhaar	
8.	1734	588	Cyber Attack	2(210)/17-Parl.	GC(AK)	
9.	-	604	Webpage for Grievance Redressal	2(235)/17-Parl.	JS(RB)	
			Regarding GST			
10.	1993	612	Semi-conductor manufacturing unit	2(216)/17-Parl.	GC(DD)	
11.	-	618	IT in Rural Areas	2(236)/17-Parl.	JS(SM)	
12.	2454	652	Cashless Economy	2(220)/17-Parl.	JS(RB)	
13.	1548	656	Job Losses in IT Sector	2(219)/17-Parl.	JS(RK)	
14.	-	673	Losses due to Cyber Attack	2(234)/17-Parl.	GC(AK)	

The following questions have been admitted for answer in Lok Sabha on 19.07.2017 (Wednesday).

There is No Starred Question in Lok Sabha on 19.07.2017.

2. Draft Reply must be typed in double space. File containing the answer to Questions please be submitted latest by 13.07.2017 for onward submission to Hon'ble Minister, MeitY / Hon'ble MOS, MeitY.

3. Use of abbreviations may be avoided and in case they are used, their full form may also be given in the brackets. It has been observed that illegible photo copies of annexure are appended some time. It is, therefore, requested that either original copy or neat, clean or legible copy of the annexures/enclosures may be attached. Further, it is also requested that a soft copy of the Note for Supplementaries prepared for Starred Questions may please be forwarded to the PS to Hon'ble Ministers at: mljoffice@gov.in and PS to Hon'ble MOS at: mos-mlj@meity.gov.in and ravi.raghav@meity.gov.in.

4. If reply to any question contains long annexure/tables, etc. such information may please be provided to Parliament Section through USB for facilitating their accurate and speedy translation in Hindi. Alternatively it may be **e-mailed.**

(Vinodpriya) Section Officer(Parl.)

Deputy Director(Parl.)

Concerned GCs

- Copy to: 1. Minister's Office
 - 2. MOS's Office
 - 3. Secretary's Office, MeitY
 - 4. Senior Economic Adviser (Parl.), MeitY
 - 5. OSD to MOS