finalize an arrangement within 2018 to enable the export of Canadian pulses to India free from pests of quarantine importance, with mutually acceptable technological protocols.

(b) and (c) As per the 2nd Advance Estimates, 2017-18, released by the Department of Agriculture, Cooperation and Farmers Welfare, the estimated production of pulses is 23.95 million tonnes in 2017-18 and 23.13 million tonnes in 2016-17 (Final Estimates). Pulses from buffer is released to States/UTs, Central agencies or through open market sales based on demand and exigencies.

2492. *[The Question was cancelled.]*

Misuse of Aadhaar data

2493. DR. PRADEEP KUMAR BALMUCHU:
SHRI T.G. VENKATESH:
SHRI DHARMAPURI SRINIVAS:

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

(a) whether it is a fact that the Aadhaar data is being misused and following the complaints, Aadhaar servers have stopped their services across the country recently;

(b) if so, the details thereof and the reasons therefor;

(c) whether the Government has investigated the matter, and if so, the details thereof; and

(d) the remedial steps being taken by the Government to resolve the problem once and for all?

THE MINISTER OF STATE IN THE MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI K. J. ALPHONS): (a) to (d) No, Sir. The data of resident collected during enrolment gets encrypted as soon as the enrolment takes place thereby diminishing the possibility of any misuse of the data. Ensuring security of data is a continuous exercise and Unique Identification Authority of India (UIDAI) has deployed state of art security measures and continuously upgrading it as per requirement.

Cyber security professionals

2494. PROF. M.V. RAJEEV GOWDA: Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether the target of five lakh cyber security professionals by 2018 has been met, as per the National Cyber Security Policy, 2013;

(b) if so, the details thereof; and

(c) if not, the reasons therefor?

THE MINISTER OF STATE IN THE MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI K. J. ALPHONS): (a) to (c) National Cyber Security Policy, 2013 envisaged for creation of a workforce of five lakh cyber security professionals in the next five years through capacity building, skill development and training. The capacity building is a continuous process.

Ministry of Electronics and Information Technology (MeitY) has taken following initiatives for capacity building in the area of cyber security:–

(i) Under the Information Security Education and Awareness (ISEA) Project Phase-I (2005-2014), more than 44,000 candidates were trained in various formal/non-formal courses in Information Security through 40 institutions (including IISc. Bangalore, TIFR Mumbai, 4 IITs, 15 NITs, 4 IIITs, 7 Government Engineering Colleges and select centres of CDAC/NIELIT). Around 100 Government officials, covering NIC, ICERT, STQC, CDAC, NIELIT, ERNET, Scientists from MeitY, etc. were trained as Master Trainers in the area of Information Security. The ISEA Project Phase-II project aims to train more than one lakh candidates in various formal/non-formal courses and more than 13,000 Government officials by March, 2020.

(ii) Further, 28,069 candidates have been trained/under-going training in various formal/non-formal courses through 52 institutions and 4,457 Government officials have been trained in various short term courses in the area of Information Security. Besides this, 606 half day general awareness workshops on Information Security have been organized across the country for various user groups covering 65,342 participants.

(iii) MeitY in collaboration with Data Security Council of India (DSCI), has set up Cyber Forensic Labs at Mumbai, Bengaluru, Pune and Kolkata for awareness creation and training programmes on cyber crime investigation. 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. Mumbai, Pune, Bangalore

and Kolkata and in North-Eastern States at respective Police headquarters to train LEA officials (Police) in cyber crime detection. Using these facilities, more than 28000 Police/LEA personnel have been trained.

(iv) Further, cyber security is increasingly getting introduced in curriculum of schools and colleges every year. Many universities and institutions are offering Ph.D. and Master degree specializing in Cyber Security/Information Security. Vocational training program on cyber security have been introduced by Ministry of Skills Development and Entrepreneurship, as well as in universities like IGNOU.

Cyber crisis management plan for curbing cyber fraud

2495. SHRI BHUBANESWAR KALITA: Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether it is a fact that several cases of internet frauds have come to the notice of Government;

(b) if so, the details thereof during the last three years;

(c) whether it is also a fact that the Government has drawn a Cyber Crisis Management Plan to check cyber frauds in the country; and

(d) if so, the details thereof along with the achievements of the plan, so far?

THE MINISTER OF STATE IN THE MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI K. J. ALPHONS): (a) and (b) As per incidents reported to the Indian Computer Emergency Response Team (CERT-In), a total of 71, 63 and 77 phishing incidents affecting customers of financial organisations were reported in 2015, 2016 and 2017 respectively. In addition 14 incidents affecting ATMs, cards, Point of Sales (POS) systems and Unified Payment Interface (UPI) have been reported during the year 2017.

(c) and (d)

(i) Ministry of Electronics and Information Technology (MeitY) has formulated Cyber Crisis Management Plan (CCMP) for countering cyber-attacks and cyber terrorism for implementation by all key Ministries/Departments of Central Government, State Governments and Union Territories.

(ii) The Indian Computer Emergency Response Team (CERT-In) along with Reserve Bank of India is enabling implementation of CCMP in banks by means of cyber security framework, minimum baseline resiliency requirements and best practices/guidelines.