Dr. Sanjay Bahl
Director General

Sec(HE)
25/5/22

भारत सरकार
Government of India
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
Ministry of Electronics & Information Technology
भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सर्ट-इन)
Indian Computer Emergency Response Team (CERT-In)
इलेक्ट्रॉनिक्स निकेतन 6, सी जी ओ कॉम्पलेक्स, नई दिल्ली-110003
Electronics Niketan, 6, C G O Complex, New Delhi-110003
Tel. : 24368544, Fax : 24366806, E-mail : sanjay.bahl@gov.in

D.O. No. 20(3)/2022-CERT-In **Dated: 20.05.2022**

Sub: Cyber Security Directions and FAQs issued by CERT-In

27-5-22
JS (SS)

JS(A)

Dear Sir,

The Indian Computer Emergency Response Team (CERT-In) serves as the national agency for performing various functions in the area of cyber security in the country as per provisions of section 70B of the Information Technology Act, 2000. CERT-In continuously analyses cyber threats, handles cyber incidents and regularly issues advisories for protection of data/information and ICT infrastructure.

In order to augment and strengthen the cyber security as well as to enableOpen, Safe& Trusted and Accountable Internet in the country, CERT-In has issued Cyber Security Directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents under the provisions of sub-section (6) of section 70B of the Information Technology Act, 2000 on 28.04.2022. These directions are issued to service providers, intermediaries, data centres, body corporate and government organizations and cover aspects related to synchronization of ICT system clocks, reporting of cyber incidents to CERT-In, types of cyber incidents to be reported, maintaining logs of ICT system among others.The directions will become effective on 27.06.2022.

In this connection Hon'ble Minister of State for Electronics & Information Technology & Skill Development and Entrepreneurship Shri Rajeev Chandrasekhar released a Frequently Asked Questions (FAQs) document on 18.05.2022. These FAQs have been prepared in response to general queries received by CERT-In on the Cyber Security Directions and explains the nuances of the directions in a simple and easily understandable manner towards operationalization of these directions.

21/6/22 Sh. Rituraj

Dis (Educational Technology)
US (Tel)

The Cyber Security Directions and the FAQs released by CERT-In are enclosed for perusal and for issuing necessary directions to concerned officers for compliance.

The Cyber Security Directions and FAQs are also available on website of CERT-In at https://www.cert-in.org.in/Directions70B.jsp

With regards,

(Dr. Sanjay Bahl)

To,

Shri K. Sanjay Murthy
Secretary
Department of Higher Education
Ministry of Education

No. 20(3)/2022-CERT-In
Government of India
Ministry of Electronics and Information Technology (MeitY)
Indian Computer Emergency Response Team (CERT-In)

Electronics Niketan,
6 CGO Complex,
New Delhi-110003

Dated: 28 April, 2022

Subject: Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.

Whereas, the Central Government in terms of the provisions of sub-section (1) of section 70B of Information Technology (IT) Act, 2000 (IT Act, 2000) has appointed "Indian Computer Emergency Response Team (CERT-In)" vide notification dated 27th October 2009 published in the official Gazette and as per provisions of sub-section (4) of section 70B of IT Act, 2000 The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security:-

a) collection, analysis and dissemination of information on cyber incidents;
b) forecast and alerts of cyber security incidents;
c) emergency measures for handling cyber security incidents;
d) coordination of cyber incidents response activities;
e) issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
f) such other functions relating to cyber security as may be prescribed.

And whereas, "The Information Technology (The Indian Computer Emergency Response Team and Manner of performing functions and duties) Rules, 2013" were notified and published vide notification dated 16.01.2014 by the Central Government in exercise of the powers conferred by clause (zf) of sub-section (2) of section 87 read with sub-section (5) of section 70B of the IT Act, 2000.

And whereas, as per provisions of sub-section (6) of section 70B of the IT Act, 2000, CERT-In is empowered and competent to call for information and give directions to the service providers, intermediaries, data centres, body corporate and any other person for carrying out the activities enshrined in sub-section (4) of section 70B of the IT Act, 2000.

And whereas, various instances of cyber incidents and cyber security incidents have been and continue to be reported from time to time and in order to coordinate response activities as well as emergency measures with respect to cyber security incidents, the requisite information is either sometime not found available or readily not available with service providers/data centres/body corporate and the said primary information is essential to carry out the analysis, investigation and coordination as per the process of law.

And whereas, it is considered expedient in the interest of the sovereignty or integrity of India, defence of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence using computer resource or for handling of any cyber incident, that following directions are issued to augment and strengthen the cyber security in the country:

(i) All service providers, intermediaries, data centres, body corporate and Government organisations shall connect to the Network Time Protocol (NTP) Server of National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with NTP servers traceable to these NTP servers, for synchronisation of all their ICT systems clocks. Entities having ICT infrastructure spanning multiple geographies may also use accurate and standard time source other than NPL and NIC, however it is to be ensured that their time source shall not deviate from NPL and NIC.

(ii) Any service provider, intermediary, data centre, body corporate and Government organisation shall mandatorily report cyber incidents as mentioned in Annexure I to CERT-In within 6 hours of noticing such incidents or being brought to notice about such incidents. The incidents can be reported to CERT-In via email (incident@cert-in.org.in), Phone (1800-11-4949) and Fax (1800-11-6969). The details regarding methods and formats of reporting cyber security incidents is also published on the website of CERT-In www.cert-in.org.in and will be updated from time to time.

(iii) When required by order/direction of CERT-In, for the purposes of cyber incident response, protective and preventive actions related to cyber incidents, the service provider/intermediary/data centre/body corporate is mandated to take action or provide information or any such assistance to CERT-In, which may contribute towards cyber security mitigation actions and enhanced cyber security situational awareness. The order / direction may include the format of the information that is required (up to and including near real-time), and a specified timeframe in which it is required, which should be adhered to and compliance provided to CERT-In, else it would be treated as non-compliance of this direction. The service providers, intermediaries, data centres, body corporate and Government organisations shall designate a Point of Contact to interface with CERT-In. The Information relating to a Point of Contact shall be sent to CERT-In in the format specified at Annexure II and shall be updated from time to time. All communications from CERT-In seeking information and providing directions for compliance shall be sent to the said Point of Contact.

(iv) All service providers, intermediaries, data centres, body corporate and Government organisations shall mandatorily enable logs of all their ICT systems and maintain them securely for a rolling period of 180 days and the same shall be maintained within the Indian jurisdiction. These should be provided to CERT-In along with reporting of any incident or when ordered / directed by CERT-In.

(v) Data Centres, Virtual Private Server (VPS) providers, Cloud Service providers and Virtual Private Network Service (VPN Service) providers, shall be required to register the following accurate information which must be maintained by them for a period of 5 years or longer duration as mandated by the law after any cancellation or withdrawal of the registration as the case may be:

a. Validated names of subscribers/customers hiring the services
b. Period of hire including dates
c. IPs allotted to / being used by the members
d. Email address and IP address and time stamp used at the time of registration / on-boarding
e. Purpose for hiring services
f. Validated address and contact numbers
g. Ownership pattern of the subscribers / customers hiring services

(vi) The virtual asset service providers, virtual asset exchange providers and custodian wallet providers (as defined by Ministry of Finance from time to time) shall mandatorily maintain all information obtained as part of Know Your Customer (KYC) and records of financial transactions for a period of five years so as to ensure cyber security in the area of payments and financial markets for citizens while protecting their data, fundamental rights and economic freedom in view of the growth of virtual assets.

For the purpose of KYC, the Reserve Bank of India (RBI) Directions 2016 / Securities and Exchange Board of India (SEBI) circular dated April 24, 2020 / Department of Telecom (DoT) notice September 21, 2021 mandated procedures as amended from time to time may be referred to as per Annexure III.

With respect to transaction records, accurate information shall be maintained in such a way that individual transaction can be reconstructed along with the relevant elements comprising of, but not limited to, information relating to the identification of the relevant parties including IP addresses along with timestamps and time zones, transaction ID, the public keys (or equivalent identifiers), addresses or accounts involved (or equivalent identifiers), the nature and date of the transaction, and the amount transferred.

And whereas, the meaning to the terms 'cyber incident' or 'cyber security incident' or 'computer resource' or other terms may be ascribed as defined in the IT Act, 2000 or "The Information Technology (The Indian Computer Emergency Response Team and Manner of performing functions and duties) Rules, 2013" as the case may be.

And whereas, in case of any incident, the above-referred entities must furnish the details as called for by CERT-In. The failure to furnish the information or non-compliance with the ibid. directions, may invite punitive action under sub-section (7) of the section 70B of the IT Act, 2000 and other laws as applicable.

This direction will become effective after 60 days from the date on which it is issued.

*****

Annexure I

Types of cyber security incidents mandatorily to be reported by service providers, intermediaries, data centres, body corporate and Government organisations to CERT-In:

[Refer Rule 12(1)(a) of The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013]

i. Targeted scanning/probing of critical networks/systems
ii. Compromise of critical systems/information
iii. Unauthorised access of IT systems/data
iv. Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.
v. Malicious code attacks such as spreading of virus/worm/Trojan/Bots/ Spyware/Ransomware/Cryptominers
vi. Attack on servers such as Database, Mail and DNS and network devices such as Routers
vii. Identity Theft, spoofing and phishing attacks
viii. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
ix. Attacks on Critical infrastructure, SCADA and operational technology systems and Wireless networks
x. Attacks on Application such as E-Governance, E-Commerce etc.
xi. Data Breach
xii. Data Leak
xiii. Attacks on Internet of Things (IoT) devices and associated systems, networks, software, servers
xiv. Attacks or incident affecting Digital Payment systems
xv. Attacks through Malicious mobile Apps
xvi. Fake mobile Apps
xvii. Unauthorised access to social media accounts
xviii. Attacks or malicious/ suspicious activities affecting Cloud computing systems/servers/software/applications
xix. Attacks or malicious/suspicious activities affecting systems/ servers/ networks/ software/ applications related to Big Data, Block chain, virtual assets, virtual asset exchanges, custodian wallets, Robotics, 3D and 4D Printing, additive manufacturing, Drones

xx. Attacks or malicious/ suspicious activities affecting systems/ servers/software/ applications related to Artificial Intelligence and Machine Learning

The incidents can be reported to CERT-In via email (incident@cert-in.org.in), Phone (1800-11-4949) and Fax (1800-11-6969). The details regarding methods and formats of reporting cyber security incidents is also published on the website of CERT-In www.cert-in.org.in and will be updated from time to time.

*****

Annexure II

Format for providing Point of Contact (PoC) information by Service providers, intermediaries, data centres, body corporate and Government organisations to CERT-In

The Information relating to the Point of Contact shall be sent to CERT-In via email (info@cert-in.org.in) in the format specified below and shall be updated from time to time:

Name	
Designation	
Organisation Name	
Office Address	
Email ID	
Mobile No.	
Office Phone	
Office Fax	

*****

Annexure III

KYC Requirements

For the purpose of KYC, any of following Officially Valid Document (OVD) as a measure of identification procedure prescribed by the Reserve Bank of India (Know Your Customer (KYC)) Directions, 2016 / Securities and Exchange Board of India Clarification on Know Your Client (KYC) Process and Use of Technology for KYC vide Circular SEBI/HO/MIRSD/DOP/CIR/P/2020/73 dated April 24, 2020 / The Department of Telecom File No: 800-12/2021- AS.II dated September 21, 2021 on Self-KYC (S-KYC) as an alternate process for issuing of new mobile connections to Local and Outstation category customers, shall be used and maintained:

a. The passport,
b. The driving license,
c. Proof of possession of Aadhaar number,
d. The Voter's Identity Card issued by the Election Commission of India,
e. Job card issued by NREGA duly signed by an officer of the State Government and
f. Letter issued by the National Population Register containing details of name and address.
g. Validated phone number
h. Trading account number and details, Bank account number and bank details

For the purpose of KYC for business entities (B2B), documents mentioned in the Customer Due Diligence (CDD) process prescribed in Reserve Bank of India Master Direction - Know Your Customer (KYC) Direction, 2016 as updated from time to time shall be used and maintained.

*****