NOTIFICATION

New Delhi, the 16th January, 2014

G.S.R 20(E).- 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 Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely :—

1. **Short title and commencement.**— (1) These Rules may be called the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. **Definitions.**— (1) In these rules, unless the context otherwise requires,--

(a) "Act" means the Information Technology Act, 2000 (21 of 2000);

(b) "Computer contaminant" means computer contaminant as defined in section 43 (i) of the Information Technology Act, 2000;

(c) "Computer emergency response" means to coordinate action during cyber security emergencies, provide incident response services to users, publish alerts concerning vulnerabilities and threats, and offer information to help improve cyber security

(d) "Computer resource" means computer resource as defined in section 2(1)(k) of the Information Technology Act, 2000;

(e) "Computer security incident" means cyber security incident;

(f) "Cyber security" means cyber security as defined in section 2(1)(nb) of the Information Technology Act, 2000;

(g) "Cyber incident" means any real or suspected adverse event that is likely to cause or causes an offence or contravention, harm to critical functions and services across the public and private sectors by impairing

the confidentiality, integrity, or availability of electronic information, systems, services or networks resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource, changes to data or information without authorisation; or threatens public safety, undermines public confidence, have a negative effect on the national economy, or diminishes the security posture of the nation;

(h) "Cyber security incident" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorized access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;

(i) "Cyber security breaches" means unauthorised acquisition or unauthorised use by a person as well as an entity of data or information that compromises the confidentiality, integrity or availability of information maintained in a computer resource;

(j) "Director General" means the Director General of the Indian Computer Emergency Response Team;

(k) "Indian Computer Emergency Response Team" means the Indian Computer Emergency Response Team set up under sub-section (1) of section 70(B) of the Act;

(l) "Information" means information as defined in section 2(1)(v) of the Information Technology Act, 2000;

(m) "Information security practices" means implementation of security policies and standards in order to minimise the cyber security incidents and breaches;

(n) "National Critical Information Infrastructure Protection Centre" means the national nodal agency for protection of Critical Information Infrastructure set up under sub- section (1) of Section 70(B) of the Act;

(o) "Security policy" means documented business rules and processes for protecting information and the computer resource;

(p) "Vulnerability" means the existence of a flaw or weakness in hardware or software of a computer resource that can be exploited resulting in their adverse or different functioning other than the intended functions.

(2) Words and expressions used in these rules but not defined and defined in the Act shall have the same meaning as is assigned to them in the Act.

3. Location.— The Indian Computer Emergency Response Team (hereinafter referred in these Rules as CERT-In) shall function at Department of Electronics and Information Technology, Ministry of Communications and Information Technology and shall be located at "Electronics Niketan", 6, CGO Complex, Lodhi Road, New Delhi – 110003.

4. Authority.— CERT-In shall be a part and under the administrative control of the Department of Electronics and Information Technology, Ministry of Communications and Information Technology.

5. Functioning on 24-hour basis.— CERT-In shall function on 24-hours basis on all days of the year including Government and other holidays and the contact details of CERT-In shall be published on its website **www.cert-in.org.in** and are updated from time to time.

6. Advisory Committee.— An Advisory Committee shall advise CERT-In on policy matters and services related to cyber security to enable it to fulfill its mandated roles and functions. The Advisory Committee shall have the following composition:

(i)	Secretary, Department of Electronics and Information Technology	...Chairman;
(ii)	Representative from the Ministry of Defence	...Member;
(iii)	Representative of the Ministry of Home Affairs	... Member;
(iv)	Representative of the Ministry of Law and justice	....Member;
(v)	Representative of the Department of Telecommunications	....Member;
(vi)	Representative of the National Security Council Secretariat	....Member;
(vii)	Representative of National Critical Information Infrastructure Protection Centre	... Member;
(viii)	Representative of Indian Institute of Science (IISc), Bengaluru	.... Member;
(ix)	Representative of an Indian Industry Association, selected by yearly rotation amongst different Indian Industry Associations, without reappointment from	

the same Industry Association having a representative on the Council in the immediately preceding year ....Member;

(x) Representative of any other Ministry as and when required ...Special Invitee;

(xi) Representative of State Governments (by rotation) ... Special Invitee;

(xii) Director General, CERT-In ....Member Convener.

7. Constituency.— CERT-In constituency shall be the Indian cyber community.

8. Functions and responsibilities of CERT-In.— CERT-In shall have functions as prescribed in section 70B of the Act and those which may be assigned to it from time to time. It shall function as the trusted referral agency for cyber users in India for responding to cyber security incidents and will assist cyber users in the country in implementing measures to reduce the risk of cyber security incidents.

9. Services.— CERT-In shall broadly provide following services:—

- response to cyber security incidents;
- prediction and prevention of cyber security incidents;
- analysis and forensics of cyber security incidents;
- information security assurance and audits;
- awareness and technology exposition in the area of cyber security;
- training or upgrade of technical know-how for the entities covered under Rule 10 and sub-rule(2) of Rule11;
- scanning of cyber space with respect to cyber security vulnerabilities, breaches and malicious activities.

10. Stakeholders.— CERT-In shall interact with and seek assistance from the following stakeholders to collect, share and disseminate information and also to respond and prevent cyber security incidents, namely: :—

(a) Sectoral Computer Emergency Response Teams;

(b) Intermediaries;

(c) Internet Registry and Domain Registrars;

(d) Industry;

(e) Vendors of Information Technology products including security products and services;

(f) Academia, Research and Development Organizations;

(g) Security and Law Enforcement Agencies;

(h) Individuals or group of individuals;

(i) International Computer Emergency Response Teams, Forums and expert groups;

(j) Agency engaged for the protection of Critical Information Infrastructure;

(k) Department of Telecommunications.

11. Policies and procedures.—

(1) **Types of incidents and level of support.—**

(a) CERT-In shall address all types of cyber security incidents cyber incidents which occur or are expected to occur in the country but the level of support given by CERT-In will vary depending on the type and severity of the incident, affected entity, be it individual or group of individuals, organisations in the Government, public and private domain, and the resources available with CERT-In at that time, though in all cases a quick response with an aim to minimize any further damage or loss of information to the affected entity will be made in a shortest possible time. Resources will be assigned according to the following priorities listed in decreasing order:—

(I) threats to the physical safety of human beings due to cyber security incidents;

(II) cyber incidents and cyber security incidents of severe nature (such as denial of service, distributed denial of service, intrusion, spread of computer contaminant,) on any part of the public information infrastructure including backbone network infrastructure;

(III) large-scale or most frequent incidents such as identity theft, intrusion into computer resource, defacement of websites etc.;

(IV) compromise of individual user accounts on multi-user systems;

(V) types of incidents other than those mentioned above will be prioritised according to their apparent severity and extent.

(b) CERT-In shall endeavour to respond and present information and assistance to the affected entities to deal with cyber security incidents as appropriate and the ultimate responsibility of the security of the computer resource shall rest with owner of the computer resource.

(2) **Cooperation and collaboration.**— CERT-In shall collaborate with:—

(I) organisations within and outside the country engaged in the specialised areas in protecting and responding to cyber security incidents;

(II) organisations engaged in collection of intelligence in general, law enforcement, investigation and forensics;

(III) academia, industry, service providers and research and development institutions;

(IV) individuals or group of individuals.

(3) **Communication and authentication with CERT-In.**— The stakeholders and public at large can communicate with the CERT-In through communication systems ranging from telephone, fax, email and postal letters. The appropriate procedures will be disseminated through its website from time to time.

12. CERT-In operations.—

(1) **Incident reporting, response and Information dissemination.**— CERT-In shall operate an Incident Response Help Desk on 24 hours basis on all days including Government and other public holidays to facilitate reporting of cyber security incidents.

(a) Reporting of incidents: Any individual, organisation or corporate entity affected by cyber security incidents may report the incident to CERT-In. The type of cyber security incidents as identified in Annexure shall be mandatorily reported to CERT-In as early as possible to leave scope for action. Service providers, intermediaries, data centers and body corporate shall report the cyber security incidents to CERT-In within a reasonable time of occurrence or noticing the incident to have scope for timely action.

The details regarding methods and formats for reporting cyber security incidents, vulnerability reporting and remediation, incident response procedures and dissemination of information on cyber security shall be published on the website of CERT-In **www.cert-in.org.in** and will be updated from time to time.

(2) CERT-In shall exchange relevant information relating to attacks, vulnerabilities and solutions in respect of critical sector with National Critical Information Infrastructure Protection Centre.

13. Disclosure of information.—

(1) During the course of interaction with user community and discharging its functions CERT-In may collect and analyse information relating to cyber security incidents from individuals, organisations and computer resource. CERT-In shall follow applicable legal restrictions, orders of competent Indian courts and ethical practices with regard to disclosure of information and shall maintain reasonable controls and internal checks to maintain confidentiality of such information.

(2) CERT-In shall not disclose any information which may lead to identification of individual, group of individuals or organizations affected by cyber security incidents without their explicit written consent or orders of Indian competent courts. CERT-In shall take appropriate measures to protect such information and shall also not disclose the identity of individuals, group of individuals and organisations sharing the information and reporting cyber security incidents to it, without their explicit written consent or orders of Indian competent courts.

(3) CERT-In may share or disclose the general trends of cyber security incidents, cyber security breaches freely to assist general public for the purpose of resolving and preventing cyber security incidents and promoting awareness.

(4) Save as provided in sub-rules (1), (2) and (3) of Rule 13, it may be necessary or expedient so to do, for CERT-In to disclose all relevant information to the stakeholders, in the interest of 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 an offence relating to cognizable offences or enhancing cyber security in the country.

14. Seeking information, carrying out functions and for compliance in terms of sub-section (6) of section 70 (B) of the Act.—

(1) **Authority.**— Any officer of CERT-In, not below the rank of Deputy Secretary to the Government of India may seek information from service providers, intermediaries, data centres, body corporate and any other person for carrying out the functions provided in sub-section (4) of section 70(B) of the Act.

(2) For cyber security, CERT-In may take recourse for monitoring and collection of traffic data in accordance with the provisions of section 69B of the Information Technology Act, 2000 and Rules notified thereunder.

(3) **Format for submission of information.**— The information sought by CERT-In shall be submitted within the duration and in the format provided alongwith the communication sent for seeking the information.

(4) **Manner of seeking and submission of information.**— CERT-In may seek the information through digitally signed email, fax or registered postal mail. The information shall be submitted to CERT-In through any suitable

communication channel such as digitally signed email, fax, registered postal letters, Read only Compact Disc or Read only Digital Versatile Disc, depending upon the volume of information and as specified by CERT-In. CERT-In may also provide a secure upload facility on their server to the individual Point of Contact as defined in Rule 17.

15. Directions for compliance.— In pursuance of its mandated roles and functions as provided in sub-section(4) of section 70(B) of the Act and with a view to enhancing cyber security of the information infrastructure in the country, Director General, CERT-In shall designate, an officer not below the rank of Director to the Government of India, to issue directions or advisory to service providers, intermediaries, data centres, body corporate and any other person. Such directions or advisory for compliance shall be issued by email signed with electronic signature, fax or registered postal mail. The service providers, intermediaries, data centres, body corporate and any other person shall comply with such directions or advisories and also report to CERT-In, within the time period and the manner as provided in the direction or advisory.

16. Report of non-compliance.— In case of any non-compliance of directions within the time period by any such named service providers, intermediaries, data centres, body corporate and any other person, the concerned aforesaid officer shall submit a non-compliance report to the Director General providing details of such non-compliance within two days from the date of expiry of such directions.

17. Point of Contact.— The service providers, intermediaries, data centres and body corporate 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 by it 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.

18. Dealing with non-compliance.— All cases of non-compliance with respect to the communications seeking information under Rule 14 and directions issued for compliance under Rule 15 shall be submitted to the Review Committee constituted under Rule 19.

19. Review Committee.—

(1) A Review Committee shall be constituted by the Central Government to review the —

(a) non-compliance of the communication, seeking information under Rule 14, issued to the service providers, intermediaries, data centres, body corporate and any other person;

(b) non-compliance of the directions issued to the service providers, intermediaries, data centres, body corporate and any other person under Rule 15;

(c) terming non-compliance of directions within the time period specified under Rule 15 by any such named service providers, intermediaries, data centres, body corporate and any other person as an offence under sub-section (7) of section 70B of the Act.

(2) The Review Committee shall consist of the following:—

(I)	Secretary, Department of Electronics and Information Technology	....	Chairman;
(II)	Joint Secretary, Ministry of Law and Justice	....	Member;
(III)	Joint Secretary Level Officer, Department of Telecommunications	....	Member;
(IV)	Joint Secretary, Ministry of Home Affairs	....	Member;
(V)	Group Coordinator (Cyber Law and e-Security), Department of Electronics & Information Technology	...	Member-Convenor

The Review Committee shall meet as often as necessary.

20. Action for non-compliance of direction.— Based on the non-compliance report as submitted by the concerned aforesaid officer under Rule 16 and such direction of the Review Committee under Rule 19, the Director General shall authorise an officer of CERT-In to file a complaint before the court as provided under sub-section (8) section 70B of the Act

[F. No. 9(16)/2004-EC]

R.K. GOYAL, Jt. Secy.

Printed by the Manager, Government of India Press, Ring Road, Mayapuri, New Delhi-110064
and Published by the Controller of Publications, Delhi-110054.

Annexure

Types of cyber security incidents need to be reported to CERT-In:

- Targeted scanning/probing of critical networks/systems
- Compromise of critical systems/information
- Unauthorised access of IT systems/data
- Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.
- Malicious code attacks such as spreading of virus/worm/Trojan/Botnets/Spyware
- Attacks on servers such as Database, Mail and DNS and network devices such as Routers
- Identity Theft, spoofing and phishing attacks
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Attacks on Critical infrastructure, SCADA Systems and Wireless networks
- Attacks on Applications such as E-Governance, E-Commerce etc.