

INFORMATION TECHNOLOGY (NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTRE AND MANNER OF PERFORMING FUNCTION

11-avgb(i)] NOTIFICATION New Delhi, the 16th January, 201 \$ G.S.R. 19(E).- In exercise of the powers conferred by clause (zc) of sub-section (2) of Section 87. read with sub-section (3) Of section 70A Of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely:- I. Short title and Commencement— ITese rules may be called the Information Technology (National 'Critical Information Infrastructure Protection Centre and Manner Of Performing Functions and Duties) Rules, 2013. (2) shall come into force On the date of their public.tiOn in the Official Gazette. -2. Definitionsr— (I) In these rules, unless the context Otherwise requires, • (a) (b) (d) (0 (g) "Act" means Information Technolog Act, 2000 (21 of 2000); "Appropriate Government"" means appropriate Government as defined in clause (e) of sub-section (t) Of section 2 orthe Act; "Body Cdrporat€" means body corporate as defined in Explanation (I) to section 43A of the Act; "Critical Information Infrastrucu« means Critical Information Infrastructure as defined in Exolanation to sub-section (I) of section 70 of the Act; "Critical Sector" means sectors, which are critical to the nation and Whose incapacitation Or destruction will have a debilitating impact on national security, economy, public healthnr: safety; "Indian Computer Emergency response Team" means the Indian Computer Emergency Response Team notified under sub-section (I) of section 70B Of the Act; "Intermediary" means an intermediary as defined in clause (w) Of sub-section (I) Of section 2 Of the Act; "Nodal Officers" means officer(s) nominated by Lhe appropriate Government(s) and liis agencies, body corporates, and other entities in the designated critical sectors, Who shall inform. cooperate With and support the designated Nodal Agency or its units as and when required for the protection Of Critical Information Infrastructure and assoc iated protected systems; "Technical Centre" means technical units Of the National Critical Information Infrastructure protection Centre or critical sector(s) or of the appropriate Governments and its agencies. which shall work cohesively in synergistic manner with the Nationalai Citicai Infovrnaion Infrastructure Centre for protection of Critical Information Infrastructure. (2) Words and expressions used jn these rules but not defined anddefined in the Act shallhave the Same meaning is assigned to them in the Act. (I) National Critical Information Infrastructure Protection Centre (hereinafter referred to ag NCIIPC)ßhali be the national nodal agency designated under section of the Act in respect of Critical Information InfrastrUCtUre and shall function at the address to be notified. (2) National Critical Information Infrastructure Protection Centre shall be a part of and under the administrative control Of the National Technical Research Organisation (NTRO), (3) National Critical Information Infrastructure Protection Centre Shall function On a twenty-four-hour I-usis on all days of the year including Government holidays. The address and other contact details of NCIIpC shall bc published on its website. (4) National Critical Idformation Infrastructure Protection Centre constituency Shall be the Indian critical information infrastructure as notified by the Government from time to time and excluding those notified under the Ministry Of Defence

4. Functions and duties of the National Critical Information Infrastructure Protection Centre—The functions and duties Of the National Critical Information Infrastructure Protection Centre shall be the following, namely:- (I) National Critical Information Infrastructure Protection Centre shall function theynational nodal agency for allr measures to protect nation 's critical information infrastructure. (2) The Ndtional Critical Information Infrastructure protection Centre Shall essentially protect and deliver advice that aims to reduce the vulnerabilities Of critical information infrastructure, against cyber terrorism, cyber warfare and Other threats. (3) Identification of all critical information infrastructure elementsfirapproval by the appropriate Government for notifying the same. '86 c,z//0-2 6 THE GAZETTE OF INDIA : EXTRAORDINARY (4) Provide strategic leadership and coherence across Government to respond 10 security threats against the identified critical information infrastructure. (5) Coordinating, sharing, monitoring, collecting analysing and forecasting, national-level threats to critical information infrastructure for policy guidance, expertise-sharing and situational awareness for early warning or alerts. The basic responsibility for protecting critical information infrastructure system shall lie with the agency running that critical information infrastructure. (6) Assisting in the development Of appropriate plans,

adoption Of standard. >aring of best practices and refinement of procurement processes in respect of protection of Critical Information Infrastructure. (7) Evolving protection strategies, policies, vulnerability assessment and auditing methodologies and plans for their dissemination and implementation for protection of Critical Information Infrastructure. (8) Undertaking research and development and allied activities, providing funding (including grants-in-aid) for creating, collaborating and development Of innovative future technology for developing and enabling the growth of skins, working closely with Wider public sector industries, academia et al and with international partners for protection Of Critical Information Infrastructure, (9) Developing or Organising training and awareness programs as also nurturing and development of audit and certification agencies for protection of Critical Information Infrastructure. (IO) Developing and executing national and international cooperation strategies for protection Of Critical Information Infrastructure. (Issuing guidelines, advisories and vulnerability or audit notes etc. relating to protection Of Critical information infrastructure and practices, procedures, prevention and response in vnsullation with the stake holders, in close coordination With Indian Computer Emergency Response Team and other organisations working in the field or related fields, (12) Exchanging cyber incidents and Other information relating to attacks and vulnerabilities With Indian Computer Emergency Response Team and other concerned organisations in the field. (13) In the event of any threat do critical information infrastructure the National Critical Information Infrastructure Protection Centre may call for information and give directions to the critical sectors or persons serving or having a critical impact on Critical Information Infrastructure. Manner Of performing functions and duties.— (1b(a) The National Critical Information Infrastructure Protection Centre shall essentially undertake its task and discharge its responsibilities in close association or coordination with the respective nodal officers of the critical sectors, Indian Computer Emergency Response Team and Other organisations working in the field or related fields. (b) Prioritisation of actions against threats or vulnerabilities shall generally be based on the type, severity, affected entity and availability of resources and the methodology' for prioritization in descending order shall be as follows, namely:- (2) (c) (3) the threat or vulnerability could result in significant physical Or economic or Other damage to the national critical information infrastructure; Government property covered under critical information infrastructure, is in danger; a significant number Of Sector(s) of the national critical information infrastructure are in danger; particular sector Of the national critical information infrastructure is endangered, Communication with National Critical Information Infrastructure Protection Centre The respective nodal officers in the various critical sectors shall communicate with the National Critical Information Infrastructure Protection Centre using all appropriate or available means Of communication. The National Critical Information Protection Centre may also take suo moto cognizance Of any vulnerability/threat that comes to its notice and that affects, or can affect, the nation's Critical Information Infrastructure, and initiate suitable measures. The National Critical Information Infrastructure protection Centre shall maintain 24x7 help desk to facilitate reporting Of incidents. National Critical Information Infrastructure Protection Centre — Operations and Response National Critical Infrastructure Centre shall, in conjunction with the nodal Officers and other agencies like Indian Computer Emergency Response Team working in the field, issue advisories or alerts and provide guidance and in addressing the threats/vulnerabilities for protection of Critical Information Infrastructure. It shall, in the event of a national-level threat, play a pivotal role and coordinate the response of the various stakeholders in the area Of critical information infrastructure in close with Indian Computer Emergency Response Team. For protection Of critical information infrastructure, the National Critical Information Infrastructure Protection Centre may take recourse for monitoring and collection of traffic data in accordance the provisions or section 69B of the and the rules notified thereunder specific to critical information infrastructure and relevant to their provisions needs The powers to the National Critical Information Infrastructure Protection Centre in interception/monitoring/decryption and blocking Of cyber information (For the purpose protection Of critical information infrastructure shall in accordance with the law and as per the Standard Procedures modalities (a) be jointly developed by Ministry of Home Affairs and NITRO_ 6. Advisory Committee— (a) -former shall be Advisory Committee to advise the National Critical Information Infrastructure Protection Centre on policy matters and -usures relating to the protection of critical information infrastructure to enable it to fulfil its mandated role and functions. (b) The Advisory Committee shall consist of the following:- (vii) (viii) (xii) (xiii) (xiv) (xvi) (xvii) Chairman/Scientific Advisor. NITRO Representative of Ministry of Home Affairs Representative Of Ministry

of Law & Justice Representative Of Department Of Telecommunications Representative of Department of Electronics & IT Representative Of Department Expenditure Representative Of Ministry of Defence General. CERT-in Representative of National Security Council Secretariat Representative Cabinet Secretariat Subject Domain Experts (Nominated by the Chairman) Two Representatives from N TRO Representative Intelligence Bureau Representative of any Other Ministry as and when required Representatives from (a) industry (b) body (c) Civil Geographical Sectors of State Governments (by rotation) Director General. National Critical Information Infrastructure Protection Centre - Chairman - - - - Member - Member - Member - Member - Member - Member(s) - Member(s) - Member - Invited • Special invited • Special Invited Member Advisory Committee shall meet as often as considered (d) The Advisory Committee may Sub-committees to address any issue relating to functioning of NCII PC. T Research and development.— The National Critical Information Infrastructure Protection Centre may seek collaboration and support research and development (direct or indirect) in accordance with rules and procedures of Government in this regard from-

8 THE GAZETTE OF INDIA : EXTRAORDINARY [PART 11—SEC. (i) Government organisations or bodies, institutes, Departments, agencies or etc.; (ii) institutes of eminence within and/or outside India; (iii) body corporates and industry associations; and (iv) subject or domain experts, [F. No. 9061/2004-ECI R.K. GOYAL, Jt. Secy. 2014 2000 (2000 S.I.T.2f) 2013 (2) (Q) 2000 (2000 21) 2000 a q.T (T43 2000 2<1) -e-e-r R--i.T-, -ét 3-1411 11—uog 3. (frr& gig -Atz-i-fit-\$ 6, - 110003 5. 24- cert:in.or9, in -q-m-f 8. 70 rrg Gift-q H o 11 (2) 186 61/11/-3 10 ITIE GAZETTE OF INDIA : EXTRAORDINARY Wtd.— q-ft fäg (PART 3fi)] (-0 (11) (3) q-aM1ü æ:ré-\$r Gg\$ 12. Yzrl-å--\$-fri--qi 24 [qrrll-avg 11 gera-r, UUfrd 13. :sæt •zraröTzh \$1 gguF (4) 13 (2) (3) 14. 70 (6) (1) 70U) (4) (2) 2000 \$r mTt, t 1 aft; 16

