Draft Rules under section 70B(5) of Information Technology (Amendment) Act, 2008

THE GAZETTE OF INDIA

EXTRAORDINARY

Part II – Section 3, Sub-Section (i)

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY

(Department of Information Technology)

NOTIFICATION

New Delhi , _____, 2009

G.S.R ---- In exercise of the powers conferred by Section 87 of the Information Technology (Amendment) Act, 2008, the Central Government hereby makes the following rules, namely:

1. (1) These rules may be called the Information Technology (The Indian Computer Emergency Response Team and manner of performing functions and duties) Rules, 2009

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

2. Definitions. – In these Rules, unless the context otherwise requires,--

a) "Act" means the Information Technology (Amendment) Act, 2008;

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 communication 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 (Amendment) Act, 2008;

g) “Cyber security incident” means any real or suspected adverse event in relation to cyber security that violates an explicit or implied security policy resulting in unauthorized access, denial of service/ disruption, unauthorized use of a computer resource for processing or storage of information or changes to data, information without authorization;

h) “Cyber security breaches” means unauthorized acquisition by a person of data or information that compromises the confidentiality, integrity or availability of information maintained in a computer resource;

i) “Director General” means the Director General of the Indian Computer Emergency Response Team

j) “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

k) “Information” means information as defined in section 2(1)(v) of the Information Technology Act, 2000;

l) “Information security practices” means implementation of security policies and standards in order to minimize the cyber security incidents and breaches;

m) “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.

3. The Indian Computer Emergency Response Team (herein after called CERT-In) functions at Department of Information Technology, Ministry of Communications and Information Technology and is 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 Information Technology, Ministry of Communications and Information Technology. It shall operate under the authority delegated under the section 70(B) of the Act.

5. CERT-In is headed by a Director General. It functions on 24 hours basis on all days of the year including government and other holidays. CERT-In is located at the following address:

Indian Computer Emergency Response Team (CERT-In)
Department of Information Technology
Ministry of Communications & Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road
New Delhi - 110 003
India

The contact details of CERT-In are 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/Special Secretary, Department of Information Technology ….Chairman
ii. Representative of Ministry of Home Affairs …. Member
iii. Representative of Ministry of Law …. Member
iv. Representative of Department of Telecommunications …. Member
v. Representative of National Security Council Secretariat …. Member
vi. Representative of National Technical Research Organisation …. Member
vii. Representative of IISc, Bengaluru …. Member
viii. Representative of NASSCOM …. Member
ix. 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 Information Technology (Amendment) Act, 2008. 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:

(a) Response to cyber security incidents

(b) Prediction and prevention of cyber security incidents

(c) Analysis and Forensics of cyber security incidents

(d) Information Security Assurance

(e) Awareness and technology exposition in the area of cyber security

10. **Stakeholders**

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

i. Sectoral CERTs
ii. Intermediaries
iii. Internet Registry and Domain Registrars
iv. Industry
v. Vendors Information Technology products including security products and services
vi. Academics, Research & Development organizations
vii. Security and Law Enforcement agencies
viii. Individuals or group of individuals
ix. International CERTs, Forums and expert groups

11. **Policies and procedures**

11 (1) **Types of Incidents and Level of Support**

(a) CERT-In shall address all types of cyber security incidents which occur or expected to occur in the country. 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, organizations in the Government, public and private domain, and the resources available with CERT-In at that time, though in all cases some response 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 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 and/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 prioritized 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. The ultimate responsibility of the security of the computer resource shall rest with owner of the computer resource.

11 (2) **Cooperation and collaboration**

CERT-In shall collaborate with:

I. organizations within and outside the country engaged in the specialized areas in protecting and responding to cyber security incidents.

II. organizations engaged in collection of intelligence in general, Law Enforcement, Investigation and forensics

III. Academia, Industry, Service providers and Research & Development institutions

IV. Individuals or group of individuals

11 (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**

12 (1) **Incident Reporting and Response**

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) Who can report: Any individual, organization or corporate affected by cyber security incidents may report the incident to CERT-In. Service providers, intermediaries, data centers and body corporate shall report the cyber security incidents of following nature to CERT-In within a reasonable time of occurrence or noticing the incident:

- Repeated scanning or probing of critical computer networks and systems
- Compromise of or unauthorised access to critical computer networks, systems or information
- Defacement of or intrusion into website
- Detection of large scale propagation of computer contaminant
- Identity Theft, and phishing incidents
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) incidents

(b) Method of reporting:

Cyber security incidents and vulnerabilities may be reported to CERT-In through the following methods:

(i) Incident Reporting

Email: incident@cert-in.org.in

The contact details of CERT-In Incident Response Helpdesk are published on its website **www.cert-in.org.in.**

(ii) Vulnerability Reporting

The vulnerabilities are to be reported to the CERT-In Information Desk.

Email: info@cert-in.org.in

The contact details of CERT-In Information Desk are published on its website **www.cert-in.org.in.**

(c) Formats of Incident Report and Vulnerability Report

The detailed information regarding cyber security incident and details of affected entity are to be furnished to CERT-In in the format given in Annexure I. The vulnerability is to be reported in the format prescribed in Annexure II.

(d) Verification

CERT-In shall verify the authenticity of the report prior to determination of suitable response actions and related priorities.

(e) Acknowledgement of Incident report

After verification of incident report CERT-In will analyse the information provided by the reporting authority and confirm the existence of an incident. In case it is found that an incident has occurred, a tracking number will be assigned to the incident. Accordingly, the report will be acknowledged and the reporting authority will be informed of the assigned tracking number. This tracking number is to be used in all related correspondence with CERT-In.

CERT-In may not respond to queries or comments received by the Incident Response Help Desk which are not related to its functions.

(f) Incident Response

Following the acknowledgement of the incident reported, CERT-In will analyse the information provided therein and may ask for additional information related to

the reported security incident. Thereafter CERT-In shall initiate incident response process as may be necessary.

CERT-In shall provide technical advice to the reporting entity through email, telephone, fax or postal mail for resolving the cyber security incident.

CERT-In may not physically deploy or send any member of its staff for attending the incident response activity at the site of occurrence. The priority of assisting in responding to the incidents will be decided by CERT-In keeping in view the severity of incident and availability of resources as described in sub rule (1) (a) of rule 11.

CERT-In shall assist the reporting entity in following broad aspects of incident handling:

- Identification: to determine whether an incident has occurred, if so in analyzing the nature of such incident, identification and protection of evidence and reporting of the same.
- Containment: to limit the scope of the incident quickly and minimise the damage
- Eradication: to remove the cause of the incident
- Recovery: taking steps to restore normal operation

(g) Incident response coordination

While handling the cyber security incidents, CERT-In shall coordinate the response activities with all agencies concerned including service providers and other Incident Response teams as appropriate.

(h) Closing of incident

After successful mitigation and recovery from incident, the incident is classified as “closed” and communication to this effect shall be sent to the reporting entity and other entities as required.

12 (2) **Vulnerability Reporting and Remediation**

CERT-In shall collect and analyze information on vulnerabilities in various IT systems and devise suitable countermeasures. CERT-In shall disseminate information regarding vulnerabilities and solutions in the form of vulnerability notes and advisories through its website and to those in the mailing list maintained by CERT-In.

A vulnerability discovered or observed in a Information Technology product, Operating System or an Application Software may be reported to CERT-In in the manner and format mentioned in rule (12) (1) (b) and (12) (1) (c).

CERT-In shall analyse the information and suggest appropriate measures to mitigate the associated risk in coordination with vendors concerned.

12 (3) **Information Dissemination**

CERT-In shall make efforts to collect and analyse information on threats and vulnerabilities in various computer platforms, operating systems, applications, network devices etc and devise countermeasures to mitigate the risk.

CERT-In shall disseminate information on cyber security issues in the form of advisories, vulnerability notes, virus alerts, whitepapers and monthly security bulletins. In addition CERT-In may also publish appropriate guidelines for securing the information infrastructure from time to time.

Information on specific cyber security incidents affecting particular organization shall be shared only with Point of Contact of said organization through secure communication channel.

(a) Methods for information dissemination

The information is disseminated by CERT-In in following methods:

I. Website: www.cert-in.org.in

II. Email: Mailing list (advisory@cert-in.org.in)

III. Telephone

IV. Postal mail

12. (4) **Sharing and reporting of information on cyber security**

Any person may share and report information on cyber security to CERT-In Information Desk through following methods:

Email: info@cert-in.org.in

The contact details of CERT-In Information Desk are published on its website **www.cert-in.org.in** from time to time.

The person reporting or sharing information with CERT-In may choose to reveal his/her identity or remain anonymous. The disclosure of the information reported or shared by the person shall be governed by the provisions under rule (13).

13. **Disclosure of information**

13 (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, organizations and computer resource. CERT-In shall follow applicable legal restrictions, orders of Indian competent courts and ethical practices with regard to disclosure of information.

13 (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 the 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 organizations sharing the information and reporting cyber security incidents to it, without their explicit written consent or orders of Indian competent courts.

13 (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.

13 (4) Save as provided in sub rule (1),(2),(3) of rule 13, it may be necessary or expedient to 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 offence or enhancing cyber security in the country.

14. **Seeking information and giving directions for compliance in terms of sub section (6) of section 70 (B) of the Act**

14 (1) Purpose

For carrying out its functions prescribed in section 70 (B) of the Act, CERT-In may seek information and give directions for compliance to the service providers, intermediaries, data centres, body corporate and any other person, as may be necessary.

14 (2) Authority and delegation

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) the Act.

14 (3) Format for submission of information

The information sought by CERT-In shall be submitted within the duration and in the format prescribed alongwith the communication sent for seeking the information.

14 (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 prescribed by CERT-In.

15. **Directions for compliance**

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

16. **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 prescribed format 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.

17. **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 18. Based on the direction of the Review Committee, appropriate action may be initiated by the Director General or by an officer authorized in this behalf by the Director General.

18. **Review Committee**

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

i. non compliance of the communication issued to the service providers, intermediaries, data centres, body corporate and any other person seeking information under rule 14 ;

ii. non compliance of the directions issued to the service providers, intermediaries, data centres, body corporate and any other person under rule 15;

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

i. Secretary, Department of Information Technology …. Chairman

ii. Joint Secretary of Ministry of Law …. Member

iii. Joint Secretary, Department of Telecommunications …. Member

iv. Joint Secretary, Ministry of Home Affairs …. Member

The Review Committee shall meet as often as necessary.

19. **Protection for actions taken in good faith**

All actions of CERT-In and its staff acting on behalf of CERT-In are taken in good faith in fulfillment of its mandated roles and functions, in pursuance of the provisions of the Act or any rule, regulations or orders made thereunder. CERT-In and its staff acting on behalf of CERT-In shall not be held responsible for any unintended fallout of their actions.

Annexure I

Incident Reporting Form

<table>
<tr><th colspan="4">Form to report Incidents to CERT-In</th></tr>
<tr><td colspan="4">For official use only: Incident Tracking Number : CERTIn-xxxxxx</td></tr>
<tr><td colspan="4">1. Contact Information for this Incident:</td></tr>
<tr><td>Name:</td><td colspan="2">Organisation:</td><td>Title:</td></tr>
<tr><td>Phone / Fax No:</td><td colspan="2">Mobile:</td><td>Email:</td></tr>
<tr><td colspan="4">Address:</td></tr>
<tr><td colspan="4">2. Sector : (Please tick the appropriate choices)</td></tr>
<tr><td>Government
Financial
Power</td><td>Transportation
Manufacturing
Health</td><td>Telecommunications
Academia
Petroleum</td><td>InfoTech
Other _____</td></tr>
<tr><td colspan="4">3. Physical Location of Affected Computer/ Network and name of ISP.</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">4. Date and Time Incident Occurred:</td></tr>
</table>

Date:	Time:

5. Is the affected system/network critical to the organisation's mission? (Yes / No). Details.

6. Information of Affected System:

IP Address:	Computer/ Host Name:	Operating System (including Version/ release No.)	Last Patched/ Updated	Hardware Vendor/ Model

7. Type of Incident:

Phishing	Spam	Website Intrusion Social Engineering
Network scanning /Probing	Bot/Botnet	Technical Vulnerability IP Spoofing
Break-in/Root Compromise	Email Spoofing	Other_____
Virus/Malicious Code	Denial of Service(DoS)	
Website Defacement	Distributed Denial of Service(DDoS)	
System Misuse	User Account Compromise	

8. Description of Incident:

9. Unusual behavior/symptoms (Tick the symptoms)

System crashes New user accounts/ Accounting discrepancies Failed or successful social engineering attempts Unexplained, poor system performance Unaccounted for changes in the DNS tables, router rules, or firewall rules Unexplained elevation or use of privileges Operation of a program or sniffer device to capture network traffic; An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user A system alarm or similar indication from an intrusion detection tool Altered home pages, which are usually the intentional target for visibility, or other pages on the Web server	Anomalies Suspicious probes Suspicious browsing New files Changes in file lengths or dates Attempts to write to system Data modification or deletion Denial of service Door knob rattling Unusual time of usage Unusual usage patterns Unusual log file entries Presence of new setuid or setgid files Changes in system directories and files Presence of cracking utilities Activity during non-working hours or holidays Other (Please specify)

10. Has this problem been experienced earlier? If yes, details.
11. Agencies notified?

Law Enforcement	Private Agency	Affected Product Vendor	Other_____

12. When and How was the incident detected:
13. Additional Information: (Include any other details noticed, relevant to the Security Incident.)

Whether log being submitted	Mode of submission:

OPTIONAL INFORMATION

14. IP Address of Apparent or Suspected Source:

Source IP address:	Other information available:

15. Security Infrastructure in place:

	Name	OS	Version/Release	Last Patched/Updated
Name OS Version/Release Last Patched / Updated				
Anti-Virus				
Intrusion Detection/Prevention Systems				
Security Auditing Tools				
Secure Remote Access/Authorization Tools				
Access Control List				
Packet Filtering/Firewall				
Others				

16. How Many Host(s) are Affected

1 to 10	10 to 100	More than 100

17. Actions taken to mitigate the intrusion/attack:

No action taken	Log Files examined	Restored with a good backup
System Binaries checked	System(s) disconnected form network	Other_____

Please fill all mandatory fields and try to provide optional details for early resolution of the Security Incident

Mail/Fax this Form to: CERT-In, Electronics Niketan**,** CGO Complex, New Delhi 110003 Fax:+91-11-24368546 or email at: incident@cert-in.org.in

Annexure II

CERT- IN **VULNERABILITY REPORT FORM**		
For official use only: Vulnerability number CERT-In#		
1. Contact Information of the person reporting:		
Name:	Organization:	Title:
Office Phone: Cell Phone:	Email:	Fax Number:
Address:		
2. Date and Time of Identification:		
Date:	Time:	
3. Type of Vulnerability (check all that apply):		
Input Validation error Boundary Condition error Buffer Over Flow Access Validation Error Exceptional Condition Error	Environment Error Configuration Error Race Condition Others	
4. Common Weakness Enumeration (CWE) : *(if any)*		

5. Information of Affected System:		
Application	Operating System	Hardware
Name Version Release	Name Version Release	
6. Vulnerability Description (Attach additional sheets if required):		
7. Vulnerability Consequences:		
8. Suggested Solution:		
9. Other Agencies notified:		
10. Additional Information:		