No. 3(15)/2004-CERT-In
Government of India
Ministry of Electronics & Information Technology(MeitY)
Indian Computer Emergency Response Team (CERT-In)
'Electronics Niketan', 6, CGO Complex,
Lodi Road, New Delhi – 11003

Dated: 03.07.2017

Subject: IT Security auditing requirements of Government organizations and critical sectors – advisories reg.

1. The Indian Computer Emergency Response Team (CERT-In) under Ministry of Electronics & Information Technology(MeitY), Government of India is maintaining a list of IT security auditing organizations to assist Government organizations and critical sectors in getting their IT systems and networks audited from cyber security point of view and to enhance their security posture. These IT security auditing organizations are empanelled by CERT-In after a thorough process of skill verification involving demonstration of their technical skills to CERT-In. The credentials of these IT security auditing organizations have been vetted by Ministry of Home Affairs. Currently, the list contains 52 IT security auditing organizations and these can be accessed at CERT-In website at "www.cert-in.org.in". At present, this list is being consulted by all the Government organizations and critical sectors for their IT security auditing requirements.

2. In relation to the process of engaging the CERT-In empanelled IT security auditing organizations, on the advice of IB/MHA, it is felt necessary to issue the following advisories to ensure that the engagement process is secure and does not pose a threat to sensitive date/information belonging to the Govt. and critical sectors.

   i) Since engaging non-Indian firms for auditing requirements by the Government organizations and critical sectors may involve exposing sensitive information to non-Indian persons/entities or having foreign links, the concerned Government Ministries/Organizations should obtain NOC from MHA before engaging any non-Indian firm.

   ii) Every auditing firm and its auditors (personnel) engaged should sign Non-Disclosure Agreements (NDAs) before being allowed to commence the cyber security auditing work. To the extent feasible, it may be ensured that any data collected during the auditing work and report prepared thereof is not allowed to be taken out of the Government premises by such auditors/firms.

3. It is requested that a suitable communication may please be sent to all the Govt. organizations and critical sectors within the purview of your domain to put in place an appropriate mechanism to ensure compliance to the above advisories at the time of engaging CERT-In empanelled organizations, in the interest of security of sensitive data/information belonging to the Government and critical sectors.

(Dr. Sanjay Bahl)
Director General, CERT-In
T.No. 011-24368544
Fax: 011- 24366806

To:
1) All Secretaries of Central Government Ministries/Departments.
2) All Chief Secretaries of States & UTs.

Copy to: 1) Shri Sudhir K. Saxena, Joint Secretary (IS-I)
Ministry of Home Affairs, New Delhi

2) Shri A. Sunil Achaya,
Joint Director, Intelligence Bureau,
35, S.P Marg, New Delhi - 110021