Calling attention of CVC and CAG

Posted on April 30th, 2011
by naavi in All News, India News
Read 468 times.

I would like to bring to the notice of the Central Vigilance Commission and the Comptroller and Auditor General of India an apparent irregularity that needs investigation in the interest of the Country. The issue involves according to one estimation a decision proposed to be taken by the Ministry of communications and Information technology resulting in IT stake holders collectively spending Rs 700 crores immediately by a payment to a private party abroad just to know what is the law of Information security in India that applies to them. Stakeholders who want to comply with the law later may collectively be required to spend around Rs 30000 crores each year to follow the law as being notified and this commercial benefit is again going to private sector because of this notification.

There is a need therefore to stop the approval of the proposed notification until a national debate is undertaken in the matter and all stakeholders are convinced that there is no reason to suspect irregularity in the promotion of a commercial benefit of this magnitude.

In February 2011, MCIT had issued a draft notification regarding Section 43A of ITA 2008 for public comments. Naavi.org had raised an issue titled " Is India selling itself out to ISO 27001?

Essentially the article had pointed out that the draft guidelines on Section 43A was indirectly imposing an an "ISO Tax" on Indian corporate entities.

It was pointed out that the guideline which was proposed to be a rule under the statutory Act (ITA 2008) contained a provision which made ISO 27001 audit mandatory for all IT users to follow the prescription of "Reasonable Security Practice" as envisaged as a responsibility under the Act.

It was also pointed out that

> a) ISO 27001 is a proprietary framework not available in public domain except at a cost of around US $160.(approx Rs 7000). This meant that whoever wanted to know what the law in relation to Section 43A is, should buy a copy of the official version of the specifications involving an outgo of foreign exchange. Since referring to the specifications bought by some body else would amount to copyright

violation, every IT stake holder had to buy an individual copy of the specification. Since there could be upto 10 lakh IT stake holders in India (there are as many registered companies in India besides unaccounted number of website owners who are also stakeholders under section 43A), a sum of around Rs 700 crores would have to be invested by the Indian community just to buy copies of the ISO 27001 specification.

b) If the average cost of conducting an ISO 27001 audit is around Rs 3- 5 lakhs, the total investment for the entire community of 10 lakh stake holders to be compliant with law would be a minimum of Rs 30000 crores. This audit needs to normally be repeated once in 3 years and hence would be a recurring cost for the community.

c) At present there are not the required number of ISO auditors who can conduct ISO audits for even 10000 clients in a pace of two or three years. Hence the introduction of the rule would only create non compliant community and does not add to the security scenario.

d) It was also pointed out that ISO 27001 audit has not proved to be a panacea for security ills. In fact India is facing Cyber Crimes and insider frauds just like other countries despite many companies having already adopted ISO 27001 audits. One glance at the Indian Banking scenario indicates that ISO audit doesnot guarantee even a minimum standard of security to prevent Phishing and other frauds. The need to make such an audit mandatory and provide a national approval through a statute was therefore pointed out as highly improper.

e) The need to adopt an Indigenous information security framework which was in the public domain was therefore highlighted.

In view of the above the following clauses in the proposed rules were objected.:

7. Reasonable Security Practices and Procedures.— *(1) Any person, including a body corporate shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards which shall require a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected. In the event of an information security breach, any such person, including the body corporate shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies.*

(2) The International Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" has been adopted by the country. The security practices prescribed by this standard are enshrined in the principle outlined in sub-rule (1).

(3) Industry associations or industry cluster who are following other than IS/ISO/IEC 27001 codes of best practices for data protection and fulfil the requirement of sub- rule (1), shall get their codes of best practices approved by the government, which shall be duly notified.

(4) The body corporate who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures.

The specific objections were

a) to declare ISO 27001 as having been "adopted by the country" since this was getting enshrined as a certificate from the Indian Parliament through the notification.

b) To make the existing guidelines of different organizations including information security guidelines issued by SEBI and RBI subordinate to ISO 27001 as requiring a due notification.

c) To consider all existing ISO audited entities automatically compliant with Sec 43A requirements.

In view of the issues involved, an RTI application was sent to the MCIT to understand why the department was interested in recommending a practice which is known to be deficient in practice and would cost enormous money for compliance.

The RTI application sought the following information:

In recommending that "The body corporate who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures" as part of the draft notification "Information Technology (Reasonable security practices and procedures and sensitive personal information) Rules, 2011" (regarding Section 43A of Information Technology Act 2000), information on the estimated impact of the notification that has been taken into consideration while arriving at the recommendation such as

a) How many body corporates as defined in Information Technology Act 2000/2008 in India have so far adopted IS/ISO/IEC 27001 standard?

b) If the draft notification is brought into force, how many body corporates (which includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities) in India are estimated to adopt the said standard in the next 3 years?

c) What is the estimated cost of all the stakeholders obtaining an official copy of the standard documentation?

d) What is the estimated cost of all the stakeholders obtaining an audit certificate under the said standards?

e) What is the estimated number of auditors available in India for conducting such audits and the estimated time required if all the stakeholders do consider adopting the standards?

f) What is the ownership of the organization which manages the said standards and is there any revenue inflow to the Government of India on account of stakeholders adopting the said standards?

g) What is the total estimated cost of all stakeholders getting themselves certified for the recommended standards?

h) Were any other information security standards also considered for adoption and rejected in preference for the said standard and if so what were the considerations for which the said standards were preferred?

And if such information has not been taken into consideration, what other criteria has been used to arrive at the recommendation.

A reply was received from the department on 25th March 2011 which stated :

a) 516 organizations have so far obtained ISO 27001 certification in the country as per details published on the website www.iso27001certifcates.com

b) to h). This department does not have information related to these points.

It is significant to note that the department admits that it does not know what would be the financial impact of the cost of implementing the rules to be notified by the department.

Since the article of Naavi was in public domain, the department was aware that there was on school of thought which

thought that there was a financial outgo of Rs 700 crores on the Indian community to just understand what the law is and this was considered as "ISO Tax" and also that the rule would result in a financial benefit of Rs 30000 crores for every three years (or Rs 10000 crores per year) to the ISO 27001 community at the cost of IT stake holders.

It was impreative for the department to have considered these thoughts and evaluated their proposal. The RTI reply does not indicate if any such exercise was undertaken.

In the revised notification now issued on April 11, the words "ISO 27001 has been adopted by the country" has been removed. But the recognition that companies which have conducted ISO 27001 audit will be deemed to have complied with ISO 27001 remains with an addition that the audit should be annual.

Now in the finalized rules therefore, it appears that the department is pushing this ISO levy of Rs 700 crores and commercial benefit of Rs 30000 crores per annum to the private bodies.

The sequence of events donot provide the confidence to the citizens of this country that the decision taken by the MCIT in framing the rules under Section 43A are based on proper evaluation of its consequences and there is a primafacie doubt if the decision was influenced by the ISO 27001 lobby for serving their vested interests.

I therefore urge the department to withdraw the notification failing which I urge the CVC and the CAG to examine if the decision is not influenced by any non professional considerations.

Naavi of Naavi.org

Let Others Know About This Post These icons link to social bookmarking sites where readers can share and discover new web pages.

Click Below To Rate This Post:

 (**1** votes, average: **4** out of 5)

Loading ...

No user commented in " Calling attention of CVC and CAG "

Follow-up comment rss or Leave a Trackback

Leave A Reply

Username (*required)

Email Address (*private)

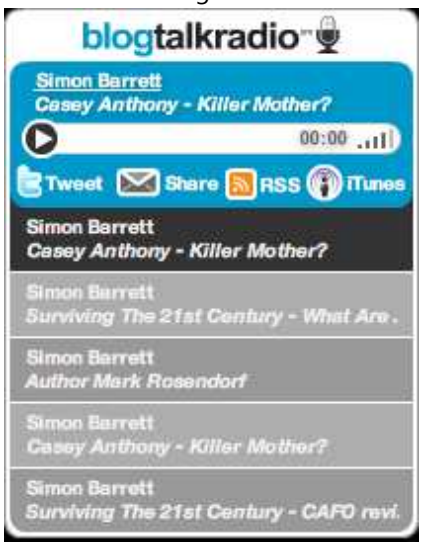
Website (*optional)

Post My Comment

Advertisements:

BloggerNews On The Air

We are pleased to announce our latest endeavor, Blogger News is now sponsoring some radio shows on Blog Talk Radio. You can check our full schedule, and listen to previous broadcasts here, and we hope that you will join us on the air in this new venture.



Hot Topics, In-Depth:

While BloggerNews.net is known to provide up to the minute information on a wide variety of topics, at times a more in-depth analysis of a topic that is being written about by our writers is warranted. This section of BNN provides just that – an area of the site that looks deeper into a topic, delves into the actual facts behind it, and provides more than just a summary overview of what is happening right here and now.

From something as mundane as an overview of how credit scores work, to life and death topics such as mesothelioma, we are committed to creating a growing library of information for our readers. Click below to review the topics covered so far, and check back soon as new ones are to be added regularly!

Click Here to Review our 'Hot Topics, In-Depth' section.

Recently Published Topics, by category:

Health: Mesothelioma

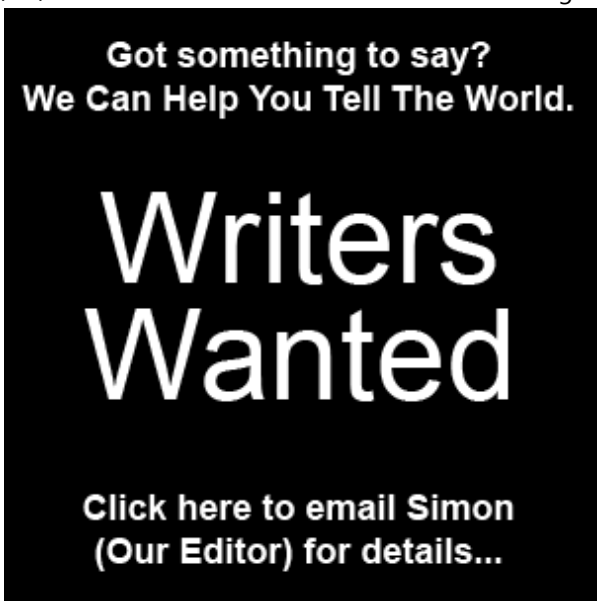
Friends Of Blogger News

BNN would like to recognize these two individuals for the enormous help they have provided us in our investigations

TJ Hart News Director for The Sky 97.3 News Talk Radio

Investigator William Cobra Staubs, Bill comes through when others do not.

BloggerNews.net Wants You!



Recent Entries

- Bloggernews.net blocked in India?
- Some Basic Facts about the FDA and How it Fails to Protect Americans from the Dangerous Effects of Drugs and Foods like Genetically Modified Foods, Dangerous Chemical Ingredients and Meat from Factory Farms
- 5 Tips to Avoid bin Laden Scams
- Spring Is In The Air (And So Are Dating Scams)
- The febrile world of British politics
- Misunderstandings about the military
- Casey Anthony – Radio Update May/8
- British psychologists warn of 'causal link' between internet porn and rise in sex offences
- Governor of RBI needs to clarify..
- Casey Anthony – Perry 1 Press 0 – BNN On The Radio

Similar Posts:

- ISO Tax on Indian Corporates?
- Indian Information Security Framework under ITA 2008
- Legal Compliance Requirements in Information Security Audit in India
- LIPS, Indian answer to USPTO Concerns
- Are You ITA 2008 Compliant?

May 2011

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

« Apr

Archives

- May 2011
- April 2011
- March 2011
- February 2011
- January 2011
- December 2010
- November 2010
- October 2010
- September 2010
- August 2010
- July 2010
- June 2010
- May 2010
- April 2010
- March 2010
- February 2010
- January 2010
- December 2009
- November 2009
- October 2009
- September 2009
- August 2009
- July 2009
- June 2009
- May 2009
- April 2009
- March 2009
- February 2009
- January 2009
- December 2008
- November 2008
- October 2008
- September 2008
- August 2008
- July 2008
- June 2008
- May 2008
- April 2008
- March 2008
- February 2008
- January 2008
- December 2007
- November 2007
- October 2007
- September 2007
- August 2007
- July 2007
- June 2007
- May 2007
- April 2007
- March 2007
- February 2007
- January 2007

- December 2006
- November 2006
- October 2006
- June 0