TAKSHASHILA
INSTITUTION

POLICY ADVISORY
May 11, 2011

Comments on

"Discussion Draft on National Cyber Security Policy"

Rohan Joshi & Srijith K Nair

EXECUTIVE SUMMARY

The Department of Information Technology, Government of India issued a discussion draft on National Cyber Security Policy (termed 'the draft' here on) on 26th March 2011 and invited comments on it. In our opinion this draft of the national policy is a considerable initial step and the government should be commended for being attuned to the threats and challenges facing the management of cyberspace and taking steps to address them. We feel that the document substantially addresses several areas and processes related to cyber security, particularly incident response, vulnerability management and infrastructure security.

However, we have identified some areas of improvement, including scope, ownership, resource allocation and management, technical and non-technical controls, which we present for the government's consideration. This document provides comments and feedback on the draft.

Rohan Joshi is Fellow for Cyber Security at the Takshashila Institution and a cyber security professional. Email: rohan@takshashila.org.in

Srijith K Nair is Fellow for Cyber Strategy Studies at the Takshashila Institution and an information security professional. Email: srijith@takshashila.org.in

The Takshashila Institution is an independent think tank on strategic affairs contributing towards building the intellectual foundations of an India that has global interests. http://takshashila.org.in

This document is the institution's formal response to the Government of India's discussion draft.

BACKGROUND

The Department of Information Technology, Government of India issued a discussion draft on National Cyber Security Policy[1] (termed 'the draft' here on) on 26th March 2011 and invited comments on it. This document provides comments and feedback on the draft.

The next section provides high level comments on the issued raised and discussed in the draft. This is followed by a detailed analysis of the various sections of the draft document in the next section.

HIGH LEVEL COMMENTS

The draft provides a well articulated and comprehensive policy of cyber security as it relates to Indian interests. In our view the revision of the draft must address the following considerations:

1. **Reporting and Ownership**. Is there a clearly-defined entity within the Government of India that owns cyber security as a subject? Many of the security provisions outlined in the draft are theoretically impeccable, but unless the document addresses the critical elements of ownership, mandate and empowerment, issues of the past will continue and there will be a disconnect between our intent and our capability. The draft does not provide any clarification on this fundamental ownership ambiguity. **It is important that *a single body* be identified to own cyber-security in India,** be adequately staffed and have the mandate to enforce policy, as required. The responsible entity ought to be clearly identified and its governance responsibilities, mandate and reporting structure need to be clearly spelled out.

2. **Staffing and Resources**. The draft envisages an ambitious project, which can only be successful if it has **full commitment** at the highest levels of the government, adequate and well-qualified resources, buy-in from central/ state-level entities and private sector, and adequate funding, all of which need to be sustainable over time. The document does not provide any details about these issues.

3. **Orphan Policy.** Cyber security cannot be considered in a silo. Cyber security – the business of safeguarding a country's networking and technology infrastructure, and electronic information – is a subset of national security and a cyber security policy must be congruent to a

[1] See http://www.mit.gov.in/sites/upload_files/dit/files/ncsp_060411.pdf

national security policy. However, as India does not have a national security policy, the cyber security policy identified in the draft is effectively a "policy orphan." As a result, significant gaps could exist between this policy document and what different ministries, departments and agencies assume might be India's national security goals and priorities. While we agree that this is not something that can be remedied at one go, **the orphaned nature of the cyber security policy should be recognised** and its implication studied and understood.

4. **Information Lifecycle Control**. While the draft does well to design adequate controls over some "states" of information, it is advisable to **consider the entire "information lifecycle"and design appropriate controls.** This encompasses the creation, processing, storing, transmitting/ receiving and deleting of information. Further, it is important to consider both technical controls (which the draft discusses well) and non-technical controls (which appear in limited form in the draft), because electronic information can be breached with or without the aid of technology. For example, social engineering attacks such as phishing and pretexting, and other malicious activities such as dumpster diving cannot be addressed purely through technical controls. Training and awareness programs are far more critical than pure technical controls in some states of the information lifecycle.

5. **Scope Questions**. It is advisable that the draft also **cover standards around physical security of technology and infrastructure, and hosting centres.** Periodic assessments carried out to validate compliance of technology infrastructure must include an assessment of compliance to physical security standards.

In addition, as the key stakeholders go through the exercise of classifying critical infrastructure as per this draft's requirements, will they also consider technology infrastructure in the Nuclear, Chemical, Biological and Radiological (NCBR) space? Further, does this draft envisage including the armed forces in its target audience? While mention of the armed forces is absent in *section 1.3*, Defence is listed in this draft's list of critical sectors in *section 3.3(1).*

If NCBR and military sectors are within the scope of the document, it would be prudent to show how a mandate for these sectors exists for DIT. While it is understandable if these sectors are out of scope, (given the level of sensitivity, cyber-security requirements in the military/NCBR space will be considerably

higher), it would be advisable for these scope limitations to be properly documented to avoid any future confusion about scope and ownership. This is especially relevant given recent discussions about recent incidents such as Stuxnet.

DETAILED COMMENTS

The detailed comments are with reference to specific points covered in the draft and the reference in the draft is identified by *italics*.

Section 1.4 Securing cyber space – Key policy considerations: Attribution is a complicated problem that does not have a clear solution, even with a large amount of resources at ones disposal. Giving the issue of attribution such prominence in a national security cyber policy seems inappropriate. The policy document should instead propose means to work in an environment where attribution remains a murky issue.

The same subsection considers the philosophy that security needs to be built-in from the conceptual design stage. It is encouraging that such a stance is taken in the draft but it would be good to also explain salient points on how one would tackle the security of technologies and processes that were not built with this attitude on security.

Section 2.2 International cooperation: International co-operation is indeed an imperative. But this draft should elaborate on areas in which such cooperation is envisaged and thus scope out such collaboration space.

Section 2.4 Priorities for action: (third bullet) In this draft's definition of "gateway, " clarification may be needed on how this is different from the rest of the network components to warrant a separate discussion in this document

Section 3.1 Security threat and vulnerability management: Regarding "Key actions" (4), clarification is required on who defines whether a product is "secure" or not? Are the "legally binding agreements" being discussed here above and beyond the IT Act and other legal bills being passed by the government? If so, who has oversight over these agreements?

Section 3.1 Security threat and vulnerability management: Regarding "Key actions" (5), are CERT-In and DIT the identified national security organization? If so, the "identification" part of the job has already been performed by the draft itself and as such the wording of the point should be changed to reflect this finality to this identification step.

Section 3.1 Security threat and vulnerability management: Regarding "Key actions" (7), what does the government envisage the verification process to be? Would they be in the form of mock drills, audits or via other means? Clarification on this would be helpful to readers and key stakeholders.

Section 3.2 (a) National cyber alert system: Regarding point (1), while it is good to have a wide variety of institutions involved in the National Cyber Alert System, their integrity and ability to withstand targeted compromise should be considered and responsibilities should be distributed in such a way as to reflect these capabilities.

Section 3.2 (b) Sectoral CERTS: More clarity is sought on the scope of sectoral CERTs. Would they be restricted to Central sectors or are state-level sectors also within the ambit of this draft?

Section 3.2 (c) Local incident response teams: Clarification is sought on the mandate of the incident response teams. Are they restricted primarily to government organisations or do they include private sector as well? If it is the latter, then the roles of these incident response teams and those of the private sector need to be clearly spelled out. Thought should be given to whether these incident response teams would have the necessary bandwidth and technological expertise to operate with such a broad scope.

Section 3.3 (i) (a) Implementation of security best practices in Govt. and Critical sectors: Annual awareness training for those tasked with handling critical cyber infrastructure must be made mandatory. Annual certification vs. non-certification data for these organisations must be reported to nodal agencies.

Section 3.3 (i) (a) Implementation of security best practices in Govt. and Critical sectors: With respect to point (1), we note that this is a critical step and it is encouraging that such a function is envisaged by this draft. To ensure the effectiveness and independence of this function, we feel it is advisable that the CISO not have operational IT functions to avoid potential segregation-of-duties issues, or report directly to IT groups. The function of CISO must include not only security assessments, but also incident/issue reporting and remediation. In addition, clarification is sought on why the CISO is not delegated to work with the sectoral CERTs but with CERT-In directly? Shouldn't sectoral CERTs be assigned this communication responsibility, strengthening its otherwise marginal role?

Section 3.3 (i) (a) Implementation of security best practices in Govt. and Critical sectors: With respect to point (4), there is ambiguity on the prescribed nature of

tests ("Penetration Testing, Vulnerability Assessment") and actual tests being performed ("Application Security Testing, Web Security Testing") , resulting in key areas such as system security testing, network security testing etc. not being included in the scope of the tests envisaged. If this list is meant to be non-exhaustive, it needs to be indicted in the document.

Section 3.3 (i) (b) Government networks: Clarification is sought on why the policy of a paper-less office is put forward in the draft on national cyber security? An explanation would help clarify the associated steps that would be kept in mind when implementing such directives.

Section 3.3 (ii) (b) Endorsing actions: Clarification is sought on why the endorsing action of evaluation and certification is confined to security products? Shouldn't this be expanded to all technology products being used within the Government of India's network and systems and within the critical infrastructures? For example, a network router is typically not considered as a security product but performs a vital role in securing the network. Shouldn't it be also subjected to evaluation and certification? In addition, it is our view that an annual certification of compliance with necessary cyber laws/ standards must be required for nodal agencies and ISPs. Penalties for non-compliance must be clearly defined. Furthermore, independent audits of organisations that maintain and use critical cyber infrastructure must be required to assess compliance to standards outlined in this document.

Section 3.3 (ii) (c) Data security and privacy protection for 'Trust and Confidence': Clarification is sought on why data security and privacy protection is relegated to a responsibility borne by the business entities. Shouldn't it also be the responsibility of the government since it handles citizen data? In addition, clarification is sought on why there is no attempt to provide minimum expectations in this regards by expressing the intention to have in place legal frameworks like the European Data Protection Directive?

Section 3.3 (iii) E-governance: Given that PKI is to perform such a key role in e-governance., clarification is sought on why there is no mention or discussion of securing the PKI in the rest of the draft? Questions like who operates and owns the security of PKI should also be clarified in this document.

Section 3.4 Security crisis management plan for countering cyber attacks and cyber terrorism: The plan does not seem to articulate the incident response process, and measures that must be followed when an attack is detected. One would have expected the plan to also include this aspect.

Section 3.5 Security legal framework and law enforcement: With regards to 3.5.1 and 3.6 (Security information sharing and cooperation), it is our opinion that while international cooperation is vital in the area of cyber security and cyber crime prevention, it should not be sought at the expense of the national cyber security's interest and should also reflect mutual recognition of partnership. It would be good for the draft to capture this sentiment.

Section 3.5.2 Combating Hi-Tech Crime/Cyber Crime: Clarification is sought on whether it is appropriate to mention cyber crime within the confines of the legal framework of this draft. If there is a mandate to cover cyber crime in this draft, a wider discussion across the document's various sections should be undertaken.

Section 4.2.3 Thrust areas of R&D: Is biometrics really part of "System Security"? From security perspective, isn't it just another form of authentication? Within this light, clarification is sought on the importance given to it. Is use of biometrics being championed in the draft? If not, a special mention of it would be misconstrued and should be removed.

Section 4.2.3 Thrust areas of R&D: Clarification is sought on what is considered a "trust worth system"? Did the author(s) mean "trust worthy system"?

Section 4.2.3 Thrust areas of R&D: Given the earlier identification of un-authorised access as one of the three basic categories of threats (Section 4.1), it would be advisable to include access management as a core research area, alongside Identity Management.

Contact Information:
The authors may be contacted over email at the addresses indicated on Page 1.
Other correspondence may be addressed to:

Mr Aruna Urs, Programme Manager
B103 - Maple
Godrej Woodsman Estate
Bellary Road, Bangalore - 560024