RECOMMENDATIONS
OF
JOINT WORKING GROUP
ON
ENGAGEMENT WITH PRIVATE SECTOR
ON CYBER SECURITY

NATIONAL SECURITY COUNCIL SECRETARIAT

Salient Features of the JWG Report on Engagement with Private Sector on Cyber Security

1. One of the primary challenges facing both government as well as industry is to ensure the security of their computer networks and systems. Cyber security cannot be achieved in isolation by either government or industry alone. It requires joint efforts and collaboration. Following discussion with representatives of the private sector on their role in enhancing cyber security, it was decided to set up a Joint Working Group (JWG), under the chairpersonship of the Deputy National Security Advisor, to work out the details of the Roadmap for cyber security cooperation that needed to be evolved. This JWG included representatives of both government and private sector.

2. The JWG had constituted five Sub-Groups to flesh out the details of such engagement. These five Sub-Groups submitted their reports to the JWG on 16 August, 2012, which thereafter finalized its recommendations.

3. Guiding Principles

The JWG has identified the following guiding principles and objectives that would underpin the public-private partnership (PPP) in cyber security:

a) Given the diverse stakeholders in cyber security, institutional mechanisms should be set up to promote convergence of efforts both in public and private domains;
b) Use existing institutions and organizations to the extent possible in both private sector and government and create new institutions where required to enhance cyber security;
c) Set up a permanent mechanism for private public partnership;
d) Identify bodies that can play a wider role in funding and implementation in the public and private sector;
e) Identify areas where both private and public sector can build capacities for cyber security;
f) Put in place appropriate policy and legal frameworks to ensure compliance with cyber security efforts;

g) Promote active PPP cooperation in international forums and in formulating India's position on global cyber security policies;
h) Establish India as a global hub of development of cyber security products, services and manpower; and
i) Promote indigenization and work on joint R&D projects to meet the cyber security needs of the country.

4. "Roadmap" for PPP on Cyber Security Issues

(1) Institutional Framework

On the basis of these guiding principles, the following coordination and oversight structure is proposed:

(a) There should be a permanent Joint Working Group (JWG) under the aegis of the National Security Council Secretariat (NSCS) with representatives from Government as well as Private Sector.
(b) This JWG will act as an advisory body and coordinate Public-Private Partnership (PPP) on cyber security.
(c) A Joint Committee on International Cooperation and Advocacy (JCICA) will be set up as a permanent advisory committee of the JWG in promoting India's national interests at various international *fora* on cyber security issues.
(d) The composition of both JWG and JCICA will be finalized in consultation with industry associations.
(e) The private sector will set up Information Sharing & Analysis Centres (ISACs) in various sectors and cooperate with the sectoral CERTs at the operational level.

(2) Capacity Building

(a) Critical shortage of cyber security professionals need to be tackled in mission mode with innovative recruitment and placement procedures along with specialized training of existing manpower. This programme may be implemented in PPP mode.
(b) There has to be a concerted effort to increase the number of cyber security professionals and equip them to efficiently meet the challenges of Cyber Security.
(c) Ministry of Communication and Information Technology (MCIT) and Ministry of Human Resource Development (MHRD) and the private sector may jointly establish a cyber security capacity building framework.
(d) Establishing a competency framework to assess skills required, identify gaps,

and devise strategies and programmes for capacity-building. This may include designing security certification schemes for IT professionals and advising cyber security related curriculum for formal sector (B.Tech, M.Tech., MBA etc).

(e) Work towards establishing a multi-disciplinary Centre of Excellence (COEs) in Cyber security areas including best practices, forensics, cyber crime investigation, studies, research and international frameworks/ institutions.

(f) MCIT and private sector should jointly run cyber security awareness campaigns for the general public, teenagers, children, etc.

(g) Ministry of Home Affairs (MHA) and MCIT may setup training facilities for training of Law Enforcement Agencies (LEAs) in cyber crime investigations and cyber forensics. Private sector may be associated with establishment of training facilities and provide basic and advanced level trainings to the LEAs.

(h) Government and private sector may fund research & development for development of indigenous cyber security products and solutions that meet international standards and address the global market.

(3) Security Standards and Audits

Given the role of security standards and audit in enhancing the level of preparedness and assurance in cyber security, the private sector would be an active partner in undertaking the following activities:

(a) Define baseline security standards and practices/guidelines for the critical sector organizations both in the public and private sectors. The standards may be developed by a MCIT led body with active involvement of the industry and academia.

(b) Define enhanced standards and guidelines for organizations that fall in the high risk category i.e. the critical information infrastructure organisations.

(c) Laying down of security standards and guidelines for acquisition of IT products and services.

(d) Develop protection profiles, capturing users' cyber security concerns, to aid the procurement of IT products as well as compliance verification of IT products prior to deployment.

(e) Work jointly towards the establishment of Institute of Cyber Security Professionals of India (similar to ICAI for CAs). This could be an autonomous institution under the patronage of MCIT.

(f) Make cyber security audit mandatory by appropriate amendment in the listing requirements under the Companies Act.

(4) Testing & Certification

The following measures may be taken for enhancing testing & certifying facilities to address the growing concerns relating to supply-chain vulnerability:

(a) Establishment of National Testing and Certification Schemes, under the supervision and oversight of appropriate empowered entities under the MCIT.
(b) While action is underway for establishment of Telecom Testing and Certification Centre in telecom sector, there is a need for establishment of an independent government certification body for IT products under the MCIT. The certification body should be separate from the testing facilities. In the interim, Standardisation Testing and Quality Certification (STQC) may be authorized as certificate issuing body for IT products.
(c) Development of skills and competence of evaluators, validators and certification body personnel for successfully running the National Testing and Certification Scheme.
(d) Establishment of private owned testing labs, duly accredited by the certification body; Government may provide the necessary incentives for the private sector for opening testing labs.
(e) Encourage active participation in the communities of interest for defining protection profiles for addressing the security requirements of specific sector.
(f) Take necessary steps to transition from a 'Common Criteria Certificate Consuming Nation' to a 'Common Criteria Certificate Authorizing Nation'.

5. Pilot projects

As the first step towards the implementation of the above recommendations, four pilot projects have been identified for early implementation:

(a) Setting up of a pilot testing lab,
(b) Conducting a test audit,
(c) Study vulnerabilities in a sample Critical Information Infrastructure, and
(d) Establishment of a multi-disciplinary Centre of Excellence (COE).

6. The permanent JWG (to be constituted) will work out the Action-Plan for implementation of the recommendations.