Discussion paper

on

"Cyber Security Controls Matrix for Procurement of Services & Solutions by Government Organisations"

I. Background and Objective

Insecure products, solutions and services lead to exposure to threats and cyber security breaches for procuring entities. Global scale incidents of SolarWinds and Microsoft Exchange are examples of how malicious actors are exploiting the supply chain in sophisticated way with wide scale impact.

Assuring cyber security as a feature of products & services and improving baseline cyber security requires ensuring security as part of procurement process, which will provide required push towards building cyber security culture. One way to achieve this objective is to leverage the purchasing power of the Government by setting up cyber security controls as part of procurement by the Government agencies (procuring entities).

Cyber Security Controls Matrix listed in section III of this document is developed as a reference list of cyber security controls along with method of verification of controls in procurement of ICT services & solutions including managed services by Government Organisations.

Building awareness in Government agencies to adopt cyber security controls as part of their procurement of ICT products & services as well as engagement with industry to put cyber security control requirements into practice is crucial for meeting the desired objective.

II. Proposed Next Steps

a. A consultation meeting on the controls matrix may be held with Industry through Data Security Council of India (DSCI) to fine tune the controls matrix and to include any appropriate suggestions from industry.

b. Controls matrix to be provided to Government e-Marketplace(GeM) and Central Public Procurement Portal (CPPP) to include at appropriate document & procurement process.

c. Circulation of controls matrix to Central Ministries & Department, States/UTs and hosting at CERT-In and MeitY websites.

d. Initially for 1-year, adoption of cyber security controls by procuring entity in procurement process may be kept as voluntary (as best practices) and after a year based on the outcomes & learning, controls may be mandate as part of all ICT related procurement by Government entities.

III. Cyber Security Controls Matrix for Procurement of Services & Solutions by Government Organisations

Government Organisations (Procuring Entities) may select & incorporate the appropriate & applicable controls from controls matrix below as part of their Bid/RFP/Tender/outsourcing for procurement of ICT services & solutions. Vendor/supplier or service provider needs to comply & should be able to demonstrate the required controls. Control Area (Column 1)) are divided into 8 categories of requirements viz. (i) Governance & Policy, (ii)Confidentiality, (iii)Availability, (iv)Regulatory Compliance, (v)Audits & Situational Awareness, (vi)Data Security, (vii)Application Security and (viii) Network Security. Column 2 of matrix list specification & requirements of the controls and column 3 provide indicative methods for verification of existence of the controls by procuring entity. Procuring Entities are also encouraged to add additional specific controls as per their risk profile & scope of services.

Table1: Controls Matrix

S.No	Control Area	Control Specification	Indicative Method of Verification
1.		Management commitment for adoption of industry recognised cyber security best practices & policies in service provider organisation including reporting of incidents & vulnerabilities to CERT-In.	Undertaking from board / top management.

2.	**Governance & Policy**	Incident reporting & response plan is defined and implemented.	Documented IR plan.
3.		Organisation shall a have designated Chief Information Security Officer (CISO).	Details of CISO.
4.		Cyber security policies and periodic security audit process is defined, established and reviewed by board/top management in an organisation.	• Minute of Meetings (MoM) of board / top management • Undertaking from board / top management
5.		Point of Contacts (PoC) to interact with procuring entity in case of any cyber security issue at either side.	Details of the Points of Contact (PoC)
6.	**Confidentiality**	Cyber security policies & technical controls comprising of Organisational, People, Physical & Technological controls, are in-place in a service provider organisation. Controls such as Encryption, Access controls, Network / application firewall.	Copy of cyber security policy & control.
7.		Subletting and outsourcing of services is not permitted.	Undertaking from board / top management

8.		Organisation data and metadata are processed securely and security measures are adopted by the organisation to safeguard the confidentiality of data & information.	Details of safeguard mechnisms.
9.	**Availability**	BCP and Disaster management plan are tested periodically and continuity of security controls is tested.	Undertaking from board / top management
10.		Establish, maintain, and document the minimum internal controls as defined by Cyber Security Audit – Baseline Requirements (CSA-BR) available on CERT-In website.	CSA-BR document of the organisation.
11.		Identify and ensure the organization complies with applicable laws and regulations.	• List of applicable laws and regulations. • Undertaking of compliance
12.	**Regulatory Compliance**	Comprehensive security audit of the organisation in respect to adoption of best practises and control.	Compliance report of the audit.
13.		Security compliance certificate like ISO/IEC 27001 etc.	Copy of compliance certificate.

14.		Compliance with CERT-In directions including reporting of incident, clock synchronization, logs retention period.	Undertaking from board / top management.
15.	**Audits & Situational Awareness**	Independent third party information security audit & periodic vulnerability assessments of services & solutions.	Certificate from third-party auditing organisation.
16.		Right to audit – Client organisation may audit the service provider or vendor organisation.	Compliance as part of tender document.
17.		Maintain cyber security situational awareness by regularly following CERT-In advisories & vulnerability notes.	Undertaking from board / top management
18.	**Data Security**	Any client data collected & processed by the organisation should be appropriately protected and if required, should be made available to procuring entity and Government security agencies.	Data security audit report from third-party auditing organisation.
19.		Visibility on suppliers & vendors of service provider	Details of supplier & vendors & annual

		including country of origin and right to audit them at least once in a year.	security audit reports carried out by them.
20.		Secure Encryption mechanism for data is employed.	Details of encryption algorithms and data handling.
21.	**Application Security**	Self-attestation by the board / top management to confirm the adoption of Secure Software Development Life Cycle (S-SDLC) for development of application or software.	• Report of security architect & application security quality control audit. • Details of security architect involved along with their qualification & certifications. • Undertaking by board/top management.
22.		Visibility of all components of software or system including Software Bill of Materials(SBOM), Open-source components, third party components, APIs, Plug-ins etc.	Detailed list of all components in form of SBOM.
23.		Defined procedure to check & validate the integrity of software releases.	• Review code signing procedures. • Details of authorised code

			signing certificate authorities .
24.		Mobile based application shall ensure confidentiality & privacy of client data by adopting techniques like secure configuration of mobile application, secure communication, secure data in-transit & in storage, proper authorization controls etc.	Audit report from third-party auditing organisation.
25.		For cloud based application or services, organisation shall adopt adequate safeguard or technology such as implementation of Zero Trust Architecture, enforcement of strict password polices, secure configuration of cloud environment, end-to-end encryption, Identity access management to prevent any data breach or data leak.	Audit report from third-party auditing organisation.
26.	**Network Security**	Right to access to logs of perimeter security devices like Firewall, IDS/IPS, network monitoring, etc. are deployed in the organization.	As part of tender compliance.

27.		Perimeter security devices such as firewall, IDS and IPS are implemented.	Make & version of solutions and logs snippets.
28.		Network segmentation and access controls are maintained.	Network architecture diagram and details of access controls mechanism.
29.		Security Monitoring & network visibility is implemented.	Report to display logs and alerts are generated, monitored, analysed and actions are taken.
30.		Controls including multi-factor authentication and secure remote access procedures and protocols implemented for teleworking.	Teleworking security controls list and details.