DRAFT

File No.1(10)/2017-CLES
Government of India
Ministry of Electronics and Information Technology

Electronics Niketan, New Delhi
Dated: <> September, 2017

NOTIFICATION

Subject: Public Procurement (Preference to Make in India) Order 2017- Notifying Cyber Security Products in furtherance of the Order

Reference: Department of Industrial Policy & Promotion (DIPP) Notification No.P-45021/2/2017 B.E.-II dated 15.06.2017

The Government has issued Public Procurement (Preference to Make in India) Order 2017 vide the Department of Industrial Policy and Promotion (DIPP) Notification No.P-45021/2/2017-B.E.-II dated 15.06.2017 to encourage 'Make in India' and to promote manufacturing and production of goods and services in India with a view to enhancing income and employment.

2. In furtherance of the Public Procurement (Preference to Make in India) Order 2017 notified vide reference cited above, the Ministry of Electronics and Information Technology (MeitY) hereby notifies that preference shall be provided by all procuring entities to domestically manufactured/ producedCyber Security Products as per the aforesaid Order. The indicative list of Cyber Security Products is enclosed at**Annexure**.

3. **Definition of Cyber Security Product**:

For the purpose of this Notification, **Cyber Security Product** means a product or appliance or software manufactured/ producedfor the purpose of maintaining confidentiality, availability and integrity of Information by protecting computing devices, infrastructure, programs, data from attack, damage, or unauthorized access.

4. **Definition of 'local supplier'of domestically manufactured/ produced Cyber Security Products**

4.1 For the purpose of this Notification, the **'local supplier'** is defined as follows:

(A) A companyincorporated and registered in India as governed by the applicable Act (Companies Act, LLP Act, Partnership Act etc.)

AND

(B) Revenue from the product(s) in the Indian geography and revenue from Intellectual Property (IP) licensing should accrue to the aforesaid company in India. The entity claiming benefits under the Public Procurement Order 2017 in addition to being an Indian registered / incorporated entity, and supplying products should satisfy the conditions of IP ownership as under:

(B)(i) Domestically manufactured/ produced Cyber Security productmeans a product, whose Intellectual Property is owned by the Indian Company (as defined above) such that it has rights to:

(a) Use and commercialize without third party consents; and
(b) Distribute; and
(c) Modify

AND

The Indian Company should demonstrate ownership of Intellectual Property associated with the product, in addition to Trademarks applicable, if any.

(B)(ii) Even in case of open source products, all the three IP ownership rights as outlined in Paragraph B(i) above should rest with the Indian entity.

(B)(iii)IP Ownership rights would need to be substantiated by adequate proof, such as (a) adequate documentation evidencing ownership(evidenced by supporting proof such as documentation related to development but not limited to IP assignments, shrink wraps, license agreements, click wraps); **OR** (b) IP registrations. It may be noted that IP registrations is not a compulsory criteria as it is not necessary to register to exercise copyright in India.

4.2**Exclusion**:

(a) Resellers, Dealers, Distributors, implementation/ support services agencies of products, who may have limited rights to IP to enable transfer of rights to use, distribute and modify.

(b) Digital content is not considered a product e.g. videos, e-books, etc.

Definition of domestically manufactured/ produced Cyber Security productand Indian Companyshould be applied in conjunction with conditions4(A) and 4(B) outlined above,and read along with the aforesaid exclusion criteria, to suppliers of products to identify Indian Product Company.

5. **Verification of 'local supplier' of domestically manufactured/ produced Cyber Security Products**

a. The local supplier at the time of tender, bidding or solicitation shall provide self-certification that the item offered meets the definition of 'local supplier' of domestically manufactured/ produced Cyber Security Products, as per Para 4 above.

b. In cases of procurement for a value in excess of Rs. 10 crores, the local supplier shall provide a certificate from the statutory auditor or cost auditor of the company (in the case of companies) that the item offered meets the definition of 'local supplier' of domestically manufactured/ produced Cyber Security Products, as per Para 4 above.

c. In case a complaint is received by the procuring agency or the concerned Ministry/ Department against the claim of a bidder regarding supply ofdomestically manufactured/ produced Cyber Security Product, the same shall be referred to STQC.

d. Any complaint referred to STQC shall be disposed of within 4 weeks. The bidder shall be required to furnish the necessary documentation in support of the domestically manufactured/ produced Cyber Security Product to STQC. If no information is furnished by the bidder, such laboratories may take further necessary action, to establish the bonafides of the claim.

e. A complaint fee of Rs.2 Lakh or 1% of the value of the domestically manufactured domestically manufactured/ produced Cyber Security Product being procured (subject to a maximum of Rs. 5 Lakh), whichever was higher, to be paid by Demand Draft to be deposited with STQC. In case, the complaint is found to be incorrect, the complaint fee shall be forfeited. In case, the complaint is upheld and found to be substantially correct, deposited fee of the complainant would be refunded without any interest.

f. False declarations will be in breach of the Code of Integrity under Rule 175(1)(i)(h) of the General Financial Rules for which a bidder or its successors can be debarred for up to two years as per Rule 151 (iii) of the General Financial Rules along with such other actions as may be permissible under law.

6. For reasons to be recorded in writing, a procuring entity may choose to procure a higher percentage of domestically manufactured electronic products than specified in the Public Procurement (Preference to Make in India), Order 2017. This would enable the procuring entities to meet their special requirements or wherever a special policy provision exists / decision is taken by the Government to meet the demand from domestic manufacturers.

7. The Notification comes into effect immediately and shall remain valid till the revised Notification is issued.

8. The Cyber SecurityProducts Notification shall also be applicable to the Domestically Manufactured/ ProducedCyber Security Products covered in turnkey/ system integration projects. In such cases the preference to Domestically Manufactured/ Produced Cyber Security Products would be applicable only for the value of Cyber SecurityProduct forming part of the turnkey/ system-integration projects and not on the value of whole project.

9. MeitY shall be the nodal Ministry to monitor the implementation of the Cyber Security Products Notification.

10. In case of a question whether an item being procured is a Cyber Security Product to be covered under the Public Procurement (Preference to Make in India) Order 2017, the matter would be referred to the Ministry of Electronics and Information Technology for clarification.

(Arvind Kumar)
Senior Director
Tel.: <>

New Delhi, Dated <<>>.09.2017

Copy to:

1. **All Ministries/Departments of Government of India**
2. **Cabinet Secretariat**
3. **PMO**
4. **NITI Aayog**
5. **Joint Secretary (DIPP), Member-Convener of Standing Committee of Public Procurement Order 2017**
6. **Comptroller and Auditor General of India**
7. **AS&FA, Ministry of Electronics and Information Technology**
8. **Internal Distribution**

(Arvind Kumar)
Senior Director
Tel.: <>

Indicative list of Cyber Security Products

Product Category
Advanced Authentication
SOAR (Security Operations, Analytics & Reporting)
Content Protection
Social Engineering
Data Loss Prevention
GRC (Governance Risk Compliance)
Security analytics
DoS and DDoS Protection / Network Security
Cloud and SaaS Security
Multi-factor Authentication Security
Big Data Analytics
Secure Access
Web Security
Antivirus/ Antimalware
Mobile Payment
Advanced Authentication
Security Incident and Event Management
LAN Security, Network Access Control , Threat Management,
Management Software for LAN Enforcers
Cyber Threat & Risk Intelligence Management

Intelligence & Tactical Operations - Intelligent Information Management System (IIMS) for Intelligence Agencies - Unconventional Conflict & Intelligence System (UCIMS) for counter-insurgency and counter-terror tactical operations - Intellistrat - an OSINT solution (open source intelligence) for tracking trends and patterns associated with events, communities, themes, issues, organisations and people on social media and the web/internet
Antivirus/Mobile Data Protection/Mobile Insurance
Web Application Firewall
Next Generation Firewall
Mobile Data Protection
Threat Management
Web Access Management
Endpoint Security
Bot Prevention
Web Security, SSL Security, Security Softwares
Identity, Authentication and Network Security
Next Generation Security Analytics
Enterprise Mobility Management, Data Loss Prevention, Mobile Data Protection, Mobile Threat Management
Advanced Authentication
Telecom Security
Exposure Monitoring / Threat Intelligence
Mobile & Web Application Security (SAST, DAST, UBA and MAST)
Static Code Analysis
Digital Forensics
Cloud Security
Identity Management

Web Access Management / (Authentication Gateway)
Digital Onboarding Manager
Smart eID Services Platform / e-Document Security
Digital Transaction Verification services /e-Transaction Security
Internet Of Things security testing software
USB attack protection
SOC
SIEM
Cloud Access Security Broker
Identity Management
User Behaviour Analytics
Identity Management
SIEM/GRC/FIM
Threat Management Advanced Authentication Web Access Management
Threat Management Advanced Authentication Web Access Management
Security Analytics, Security Orchestration, Threat Management, Cloud Security
Vulnerability Management, Vulnerability Orchestration, vulnerability scanning
Endpoint Security, situation awareness, Networksecurity, Cloud Security
Governance, Risk and Compliance Solution
Security Monitoring, End-point security, Firewall, Threat Management, Advanced Authentication, Web Access Management, Data Loss Prevention, Mobile Data Protection, Cloud Security, Antivirus/ Antimalware
Data Security

IT Security Configuration assessment of Network Devices (Firewall, Routers and Switches) , Unix Operating Systems and Web applications (Apache and Tomcat)
Scanning and Threat Management
Threat Monitoring and Reporting
Spam Free Email Solution