BSA Submission On
Draft Public Procurement (Preference to Make in India) Order 2017 — Notifying Cyber Security Products

October 26, 2017

Shri Arvind Kumar
Scientist G and Group Coordinator
Ministry of Electronics and Information Technology
Government of India
New Delhi, India 110003

Cc: Shri. Dipak Singh, Scientist G; Shri. Vinod Kumar Chouhan, Scientist C

Dear Sir,

BSA I The Software Alliance (**"BSA"**)[1] welcomes this opportunity to offer comments on the Draft Public Procurement (Preference to Make in India) Order 2017 – Notifying Cyber Security Products in furtherance of the Order (**"Draft Notification"**) issued by the Ministry of Electronics and Information Technology (**"MeitY"**) on September 25, 2017.

The Draft Notification seeks to promote a preference for the procurement of domestically manufactured or produced cybersecurity products, in pursuance of the Public Procurement (Preference to Make in India) Order, 2017 issued by the Department of Industrial Policy and Promotion (**"DIPP"**) on June 15, 2017.[2]

We are concerned that the instead of supporting the Digital India vision to ensure a 'safe and secure cyber-space', the Draft Notification might be undermining the same. The Draft Notification is neither practical nor implementable by both procuring entities and solution providers for the following reasons:

1. Unclear scope

The definition of "Cyber Security Product" under **clause 3** of the Draft Notification is extremely ambiguous and vague. Virtually all software-enabled products are now developed and deployed with the goal of "maintaining confidentiality, availability and integrity of Information." When the definition is read alongside the list of 'Product Categories' in the annexure, it leaves considerable room for broad interpretation by the 'procuring entity'[3]. Specific cybersecurity products listed in the annexure of the Draft Notification (eg:

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, Amazon Web Services, ANSYS, Apple, ARM, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, DataStax, IBM, Intel, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro and Workday

[2] 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

[3] 'Procuring entity' as defined in the 'Public Procurement (Preference to Make in India), Order 2017 issued by Department of Industrial Policy and Promotion dated June 15, 2017.

Le – Meridien
15th floor, Room 1529
Windsor Place Janpath,
New Delhi 110001
India

P : 011-497-890-66
W: bsa.org

Enterprise Mobility Management) do not align to the definition of 'Cyber Security Product' as laid out in Section 3.

If the intention or the interpretation by the procuring entity is to apply the rules of the Draft Notification to all products and software that include cybersecurity features, procuring entities may determine that they must forego not only cutting-edge cybersecurity solutions, but also other software-enabled products and services. This may delay procurement decisions and lead procuring entities to eliminate from consideration solutions that would best meet their needs

2. Definition of a 'local supplier' creates challenges with respect to compliance obligations

The conditions to qualify as a "local supplier" set out under **clause 4** of the Draft Notification pose difficulties with respect to compliance obligations in the following ways:

i. The Research and Development ("R&D") of cybersecurity products and software solutions is often global, drawing on researchers in disparate geographies. Intellectual Property ("IP") in global product and software production is typically created globally irrespective of where it is registered. Most products may also draw upon technologies protected by different IPs, including but not limited to IP licensed from third parties. It is for these reasons that **requirements such as whether a particular entity, based in a particular jurisdiction, owns or controls IP is not practical.**

ii. It is also unclear how the revenue requirement under **clause 4.1B** of the draft notification would be determined.

iii. Mandating compliance norms like in **clause 4.1B (iii) b** pushes companies to allocate time and resources for registering IP for all products that will qualify under the definition of a cyber security product. This unnecessary step increases compliance costs and creates significant hurdles in 'ease of doing business'.

3. Security is increasingly integral to product design and isolating security features to comply with local norms increases risks

Consumers of information technology ("IT") products and services are increasingly concerned about security. Accordingly, software developers implement 'Security by Design'[4], where security concerns are considered early in the Software Development Life Cycle Process and security solutions are developed, executed, and maintained throughout the lifespan of product. This approach holds true across product architecture as well as product development. This approach results in better threat response and mitigation while also minimizes security risks. In such cases it becomes impossible to distinguish between security features from the IT products and services themselves. Therefore, modifying or isolating any specific security feature from the IT product or service in order to comply with this Draft Notification will only increase the risks and vulnerabilities in the security of the product or service.

BSA recommends that procurement policies for cybersecurity products should aim to realize the vision of Digital India. To that effect, BSA suggests that procurement policies for cybersecurity products should promote a policy environment that:

A. Incentivizes investment in cybersecurity

Laws should create an environment of certainty for companies to increase investments in creating the best global cybersecurity solutions for public procurement in India and avoid policies that divert resources to compliance with local procurement mandates.

[4] Security by Design, Amazon Web Services, https://aws.amazon.com/compliance/security-by-design/

Le – Meridien
15th floor, Room 1529
Windsor Place Janpath,
New Delhi 110001
India

P : 011-497-890-66
W: bsa.org

B. Promotes cooperation amongst private and government sector

BSA encourages the Government of India to closely engage with the private sector before adopting any policies that would have a significant impact on the cybersecurity ecosystem in India and around the world. The Draft Notification should value the letter and spirit of the Framework for the US-India Cyber Relationship (**"Framework"**)[5], formalized in August 2016. The "Shared Principles" of the Framework include a commitment to *"promote cooperation between and among the private sector and government authorities on cybercrime and cybersecurity."* Securing the digital economy can only be achieved with an open market and collaboration between the public and private sectors.

C. Encourages early deployment of the best cybersecurity solutions

a) In a fast-paced environment where malicious actors are finding new ways to launch attacks on critical infrastructure, governments should ensure that procuring agencies are encouraged to deploy the **best tools available** in the global marketplace to protect their citizens from cyber threats.
b) Policies should encourage the procurement of cybersecurity products based on their **technical merits, product quality, functionality and efficacy**, irrespective of where they are developed or manufactured, or whether IP is owned or controlled locally.
c) Policies should promote implementation of **international cybersecurity standards and proven best practices** in line with the Framework commitment *"to support the development and use of international standards and best practices for technology products and services."*

Conclusion

Efforts to promote manufacturing and production of goods and services in India should be pursued in a manner that will not undermine the India's cybersecurity. We urge the GOI to reconsider the approach of the Draft Notification, rescind the proposed measures, and work with interested parties to ensure procurement policies directed toward cybersecurity products promote improved cybersecurity capabilities rather than run against it. We encourage the Government of India to avoid procurement policies that raise costs, deter investment and discourage the procurement of the most effective technological solutions by India's public sector.

BSA member companies have a **long-standing commitment to India** and we look forward to working with the Government of India on adopting cybersecurity policies which promote a safe and secure digital economy.

Thanking you.

Yours sincerely,

Venkatesh Krishnamoorthy
Country Manager- India
BSA | The Software Alliance

[5] Framework for the U.S.-India Cyber Relationship: https://in.usembassy.gov/framework-u-s-india-cyber-relationship/

Le – Meridien
15th floor, Room 1529
Windsor Place Janpath,
New Delhi 110001
India

P : 011-497-890-66
W: bsa.org