December 31, 2019

NCSS 2020 Task Force Secretariat
National Informatics Centre
Ministry of Electronics & IT

Subject: National Cyber Security Strategy Comment Submission

Dear NCSS 2020 Task Force Secretariat:

The U.S.-India Business Council (USIBC) at the U.S. Chamber of Commerce appreciates the opportunity to provide feedback on the Government of India's (GOI) draft "National Cyber Security Strategy 2020" (NCSS 2020), and seeks ongoing dialogue with the government on its development.

Cybersecurity threats and intrusions are persistent, evolving, and increasingly severe, creating significant global challenges to protect sensitive information, critical assets, the environment, and the safety of the public. USIBC prioritizes cyber risk management and the security of information and communications technologies that underpin the digital economy via risk-based, flexible, and balanced approaches. USIBC believes that multi-stakeholder frameworks should address cyber threats and risk management activities through a common international approach. Unnecessary, mandatory or sanction-based security measures degrade ongoing investments in cybersecurity, while divergence in regulatory frameworks shifts limited information security resources from risk management activities to compliance requirements.

Leverage Existing International Frameworks, Standards, and Best Practices:

When drafting the NCSS 2020, the GOI should seek to align its approach with international standards and best practices. USIBC believes that national approaches create patchworks that are not cohesive, which increase the likelihood that country-level regimes conflict with one another. Facing an increasing fragmented global regulatory landscape, companies that want to invest and participate in India's economy often confront legal challenges, lessening their ability to comply with multiple, overlapping, and duplicative security measures. Where possible, cybersecurity policies should rely on existing standards from the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), and the Economic Organisation for Co-operation and Development (OECD), both of which promote standards that fulfill your four strategic objectives: (1) enhance national and economic security, (2) ensure standards are technically sound, (3) facilitate international trade, and (3) promote innovation and competition.

Globally, an estimated 20 countries—including key Indian trading partners (e.g., U.S., U.K., Israel, Singapore, Japan)[1]— have consolidated around the approach embodied in the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (*Framework*), which was developed through an international multi-stakeholder process. Available in multiple languages, the *Framework* uses a common lexicon and a straightforward architecture that links to ISO/IEC 27103 and ISO/IEC 27001. Cyber risk is not uniform across industries, so scalable, sector-specific profiles, e.g., financial services,[2] aerospace, telecoms, et al., are essential elements of the *Framework*.

In the future, the *Framework* will link to a parallel Privacy Framework under development by cross-linking standards, compliance, and key interdependencies. Adherence to the principles and structure outlined in the *Framework* would positively increase Indian cybersecurity, while aligning India and its corporations to norms of cybersecurity, compliance, and business thereby enhancing India's ability to tap global supply chains.

---

[1] U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework International Resources. https://www.nist.gov/cyberframework/international-resources. Accessed December 4, 2019.
[2] Financial Services Sector Cybersecurity Profile. https://fsscc.org/Financial-Sector-Cybersecurity-Profile. Accessed December 4, 2019.

Promote the Free Flow of Data Across Borders

In its recent report on AI, MeitY indicated the need for the free flow of data across borders—the same is true in cybersecurity networks. For example, cyber incidents and risk management activities are international in scope and network monitoring, trends, and threat information are shared across borders. Information security professionals rely on timely access to cyber threat data (e.g., signatures, indicators of compromise, vulnerabilities) to enhance situational awareness, calibrate defensive measures, and share mitigation strategies with stakeholders. Restrictive localization regulations artificially create cyber risk by creating blind spots to timely and actionable information exchange. Accordingly, USIBC promotes risk-based approaches that permit global innovation and the free flow of data while meeting the legitimate security needs of law enforcement.

Collaborate With International Partners

Cybersecurity requirements and notification obligations that are globally aligned minimize complexities, reduce administrative burdens, and improve system security. That's why we believe collaboration with allies and partners is essential to ensure that both the U.S. and India continue to benefit from cross-border communications, content creation, and e-commerce. USIBC believes that the GOI should commit to preserve the openness, interoperability, security, and reliability of the internet. We also think that strong multi-stakeholder processes, which draw on like-minded governments, industry, civil society, and academia, ensure that internet governance resists attempts that balkanize regulations, hinder innovation, and jeopardize the functionality of the internet.

###

The Chamber appreciates the opportunity to comment and welcomes the opportunity to provide additional information surrounding our general recommendations. Please refer questions regarding the submission to Vincent Voci (vvoci@uschamber.com) or Jacob Gullish (jgullish@usibc.com).