FACT SHEET: Framework for the U.S.-India Cyber Relationship

Cooperation on cyber issues is a key component of the bilateral relationship between India and the United States. The two countries have a strategic cyber relationship that reflects their shared values, common vision, and shared principles for cyberspace. Both sides recognize the value of enhancing and further institutionalizing their broad-based cooperation on cyber issues, and in that respect, intend to complete a framework based on the following shared principles and intended forms of cooperation.

Shared principles for the U.S-India cyber relationship include:

- A commitment to an open, interoperable, secure, and reliable cyberspace environment;
- A commitment to promote the Internet as an engine for innovation, economic growth, and trade and commerce;
- A commitment to promote the free flow of information;
- A commitment to promote cooperation between and among the private sector and government authorities on cybercrime and cybersecurity;
- A recognition of the importance of bilateral and international cooperation for combating cyber threats and promoting cybersecurity;
- A commitment to respect cultural and linguistic diversity;
- A commitment to promote international security and stability in cyberspace through a framework that recognizes the applicability of international law, in particular the UN Charter, to state conduct in cyberspace and the promotion of voluntary norms of responsible state behavior in cyberspace;
- A commitment to the multistakeholder model of Internet governance that is transparent and accountable to its stakeholders, including governments, civil society and the private sector, and promotes cooperation among them;
- A recognition of the leading role for governments in cyber security matters relating to national security;
- A recognition of the importance of and a shared commitment to cooperate in capacity building in cyber security and cyber security research and development
- A commitment to promote closer cooperation among law enforcement agencies to combat cybercrime between the two countries;

- A commitment to promote, protect, and respect human rights and fundamental freedoms online;
- A desire to cooperate in strengthening the security and resilience of critical information infrastructure;

The main areas of cooperation between the two sides to advance these shared principles are expected to include:

- Identifying, coordinating, sharing, and implementing cybersecurity best practices;
- Sharing information on a real time or near real time basis, when practical and consistent with existing bilateral arrangements, about malicious cybersecurity threats, attacks and activities, and establishing appropriate mechanisms to improve such information sharing;
- Developing joint mechanisms for practical cooperation to mitigate cyber threats to the security of ICT infrastructure and information contained therein consistent with their respective obligations under domestic and international law;
- Promoting cooperation in the fields of cybersecurity-related research and development, cybersecurity standards and security testing including accreditation process, and cybersecurity product development, including further consultations on such issues;
- Elaborating and implementing practical measures that contribute to the security of ICT infrastructure on a voluntary and mutual basis;
- Continuing to promote cooperation between law enforcement agencies to combat cybercrime including through training workshops, enhancing dialogue and processes and procedures, and setting up consultations as needed;
- Improving the capacity of law enforcement agencies through joint training programs, including equipping them to draft appropriate requests for electronic evidence in accordance with the respective laws and regulations of the United States and India;
- Undertaking skill development and capacity building programs jointly in the fields of cybersecurity, efforts to combat cybercrime, digital forensics, and legal frameworks;
- Promoting the applicability of international law to state conduct in cyberspace and further exploring how it applies to state conduct in cyberspace.
- Promoting voluntary norms of responsible state behavior in peacetime, including the norms identified by the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security;
- Committing to voluntary norms under which
    - A state should not conduct or knowingly support online activity that intentionally damages critical infrastructure or otherwise impairs the use of critical infrastructure to provide services to the public,
    - A state should not conduct or knowingly support activity intended to prevent national Computer Security Incident Response Teams (CSIRTs) from responding to cyber incidents. States should also not use CSIRTs to enable online activity that is intended to do harm,
    - A state should cooperate, in a manner consistent with its domestic law and international obligations, with requests for assistance from other States in investigating cyber crimes, collecting electronic evidence and mitigating malicious cyber activity emanating from its territory.

    - A state should not conduct or knowingly support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors;

- Cooperating mutually on telecom security related issues such as telecom equipment security standards and testing, including accreditation of entities;
- Developing a common and shared understanding of international cyber stability, and destabilizing cyber activity;
- Discussing and sharing strategies to promote the integrity of the supply chain to enhance user's confidence in the security of ICT products and services.
- Continuing to promote dialogue on incident response best practices;
- Facilitating joint tabletop exercises covering priority cybersecurity scenarios to advance specific cooperation.
- Supporting the multistakeholder model of Internet governance;
- Continuing our dialogue and engagement in Internet governance fora, including ICANN, IGF and other venues, and to support active participation by all stakeholders of the two countries in these fora;
- Holding consultations and taking steps towards improving the effectiveness of transnational cybercrime cooperation;
- Strengthening critical Internet infrastructure in India;
- Working to ensure shared understanding of technology access policy, including dual use technologies sought to be controlled by either country, including through such mechanisms as the bilateral High Technology Cooperation Group.

The complete Framework for the U.S.-India Cyber Relationship, is expected to be signed within 60 days.