

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE ISRAELI CYBER DIRECTORATE OF THE STATE OF ISRAEL

AND

**THE INDIAN COMPUTER EMERGENCY RESPONSE TEAM (CERT-In)
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
OF THE REPUBLIC OF INDIA**

CONCERNING

OPERATIONAL COLLABORATION ON CYBER SECURITY

The Israeli National Cyber Directorate of the State of Israel (INCD) and the Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology of the Republic of India (hereinafter referred to as the CERT-In), hereinafter separately referred to as "Side" and jointly referred to as the "Sides";

CONSIDERING that security is an essential element of the new digital environment and that cooperative efforts are crucial in mitigating malicious acts in cyber sphere.

RECOGNISING the need to strengthen consistent and comprehensive cooperation between both Sides; and

DESIRING to further improve computer security readiness and raise awareness around the importance of keeping systems secure, and security practices and current procedures current;

RECALLING the Agreement on 'the development of cooperation in the field of industrial and technological research and development between the State of Israel and the Republic of India signed at New Delhi on 30th day of December, 1996

In light of the above mentioned, the Sides have decided to facilitate bilateral operational cooperation in the field of cybersecurity by means of this Memorandum of Understanding (hereinafter referred to as "MOU") and have reached the following understanding:

ARTICLE 1

Basic Principles

The purpose of this MOU is to enhance the cooperation between both Sides in the cyber security field and the exchange of information pertaining to the Cyber Security in accordance with the relevant laws, rules, regulations and procedures of each Side and on the basis of equality, reciprocity and mutual benefit.

ARTICLE 2

Scope of Co-operation

Both sides agree to establish and implement cooperation in the areas of their respective competence:

- (a) Establish a broader framework for future dialogue relevant to CERT activities in cyber security;
- (b) Exchange of information and best practices on cyber security incidents and response operations
- (c) Exchange experiences regarding how to build and develop the technical infrastructure of CERT;
- (d) Exchange of threat response and incident handling information, relating to each side and assist in mitigating malicious activities.
- (e) Human Resources – capacity building and exchange of experts

ARTICLE 3 Activities

In order to implement the scope of co-operation identified in Article 2, the Sides intend to cooperate under the following modalities:

- a) Watch for possible cyber incidents (e.g. Denial of Service attacks, Phishing, Malware attacks, serious scan attacks, and forgery/defacement of government web sites) in the respective cyberspace;
- b) Support each other in taking appropriate measures in order to prevent recurrence of such cyber security incidents;
- c) Exchange information on security incidents in order to prevent serious attacks and their recurrence. Direct Video Conferencing (DVC) may be held between both Sides to exchange information.
- d) Exchange assessments of the prevailing IT security trend, as observed by each organization, periodically;
- e) Organize visits of officials of two Sides on a regular basis to discuss current issues on cyber security.
- f) Invite each other to seminars/conferences held in respective countries to discuss cyber security issues;
- g) Exploring opportunities for joint research and development on cyber security technologies;
- h) Exchange contact information (email, phone and fax numbers) and secure communication system with suitable encryption for exchanging sensitive information on cyber threats and vulnerabilities;
- i) Explore the Possibility of conducting joint security drills;
- j) Any other form of Cooperation as may be mutually agreed upon.

ARTICLE 4 Expert Group

1. For the purpose of identifying and facilitating programs under Article 3, the Sides will designate one or more representatives as members of the Expert Group.
2. The Expert Group will define the scope of co-operation as set out in Article 2 above.

3. The Expert Group may hold consultations to identify and define future activities under Article 3, review activities in progress or discuss matters related to such activities. Where necessary, and by mutual understanding, the Expert Group may hold working meetings alternately in Israel and India at a mutually agreed time.
4. The composition of the Expert Group and identification of key deliverables for the Expert Group will be mutually agreed by the Sides before each meeting of the Expert Group.

ARTICLE 5 Ways of Cooperation

1. All cooperative activities under Articles 2, 3 and 4 of this MOU will be in accordance with the domestic law, policies, rules and regulations related disclosure of information of both sides.
2. All cooperative activities under Articles 2, 3 and 4 of this MOU will be subject to the availability of funds and other resources of both Sides.
3. Unless otherwise agreed between both sides, each side will provide adequate resources adequate to carry out its own activities under this MOU.

ARTICLE 6 Intellectual Property Right

1. The Sides respect intellectual property, laws including copyright, trade secret and patent laws in the implementation of their activities. In the course of carrying out the activities within this MOU, if a Side requires to use the background intellectual property right of the other Side, a written consent from the owner for its use will be needed, unless a consent is not required by the domestic law governing that activity.
2. If not otherwise agreed by the Sides in this MOU, the Sides understand and agree that no intellectual property or associated rights of a Side will be transferred or registered to other Side under this MOU, irrespective of whether that Intellectual Property right is granted registration or not.
3. Should the activities under the MoU give rise to intellectual property rights, the Sides shall enter into separate agreement that will specifically provide for allocation of ownership and may provide for arrangement for commercialization of such rights in line with rules and regulations of each Side and the other multilateral agreements to which both Sides are party to.
4. All proprietary Confidential Information shall remain the property of the disclosing Side. The Sides agree that this MoU and the disclosure of the Confidential Information do not grant or imply any license, interest or right to the Recipient in respect to any intellectual property right of the other Side.

ARTICLE 7 Exchange/Disclosure of Information

For the purpose of this MOU:

"Traffic Light Protocol" is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colours to indicate expected sharing boundaries to be applied by the recipient(s).

Neither Side will disclose nor distribute to any third party any information transmitted by the other Side in the process of cooperative activities under this MOU, except with the prior written consent

of the other Side, unless otherwise provided by law. The Sides will not use the information for purposes other than that specified without the prior written consent of the other Side.

1. Where national security, classified, operationally or proprietary sensitive information is to be disclosed, the Side providing the information is responsible for ensuring that such information is marked accordingly, including the Traffic Light Protocol and that guidance is provided to the receiving Side on handling and protection requirements. Each Side will respect requests made on handling and protection requirements regarding the security or sensitivity of the material.
2. The Sides will respect any condition, restrictions or caveat indicated by the other Participant in respect of the handling or disclosure of information.

ARTICLE 8 Settlement of disputes

Any disputes between the sides arising from the interpretation or implementation of this MOU will be settled amicably through consultations between the Sides

ARTICLE 9 Notices and contacts

1. Any notice or other communication to be given or made under this MOU will be addressed and sent to the following contact points or to such other address as any Side may designate by notice to the other Side:

CERT-IL	
Point of Contact	Karine Ben Simhon
Position Title	Head of International Cooperation
Phone (business hours)	+972 72 3990844
Phone (after hours)	+972 72 3990801
Mailing address	77 Ha'energia street Be'er Sheva
Fax	
Email	karineb@cyber.gov.il
Alternative Contact (if 1 st POC cannot be reached)	24/7 Incident Management Center
Phone	+972 72 3990801
Email	team@cyber.gov.il

CERT-In	
Point of Contact	Dr.Sanjay Bahl
Position Title	Director General, CERT-In
Phone (business hours)	+91-11-24368544
Phone (after hours)	+91-11-24368552
Mailing address	Ministry of Electronics and Information Technology, Electronics Niketan, 6 CGO Complex, Lodhi Road New Delhi-110003
Fax	+91-11-24366806
Email	sanjay.bahl@gov.in
Alternative Contact (if 1 st POC cannot be reached)	Mr. S.S.Sarma, Scientist-F/Director, CERT-In

Phone	+91-11-24368552
Email	ss.sarma@meity.gov.in, sarma@cert-in.org.in

2. The Sides may announce a change of the contact person by notice to the contact person of the other Side. The Side may appoint separate or several contact persons for certain notices.

ARTICLE 10 Modifications

This MOU may be modified as may be required from time to time by mutual written consent of the Sides.


ARTICLE 11 Validity

1. This MOU will come into effect on the date of its last signature by the Sides and will remain in effect for a period of three (3) years unless terminated by either Side giving three (3) months' notice in writing to the other Side.
2. This Memorandum may be renewed by mutual written consent of the Sides.
3. The termination of this MOU will not affect co-operative activities under Articles 2 and 3 which are already in progress and until its completion, unless the Sides mutually determine in writing otherwise.

In witness whereof, the undersigned, being duly authorized thereto by their respective Sides, have signed this Memorandum of Understanding.

For and on behalf of

Israel National Cyber
Directorate



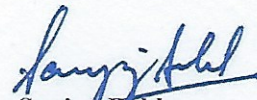
Mr. Yigal Unna
Director General
Israel National Cyber directorate

Date: 15/7/20

Place: TEL AVIV

For and on behalf of

The Indian Computer Emergency
Response Team (CERT-In),
Ministry of Electronics and Information
Technology of the Republic of India



Dr. Sanjay Bahl
Director General
Indian Computer Emergency Response
Team (CERT-In)

Date: 12 MAY 2020

Place: NEW DELHI

NON – BINDING EXPERT GROUP

NAME	DESIGNATION
CERT-In	
1. Dr. Sanjay Bahl	Director General, CERT-In
2. Mr. S.S. Sarma	Scientist 'F'/Director, CERT-In
Israel National Cyber Directorate	
1. Mr. Yigal Unna	Director General
2. Ms. Karine Ben Simhon	Head of International Cooperation