

## **MEMORANDUM OF UNDERSTANDING**

**Between**

**The Israel National Cyber Directorate of the State of Israel and the Institutional Security Cabinet of the Presidency of the Republic of Brazil  
On Cooperation in the Area of Cyber Security**

The Israel National Cyber Directorate of the State of Israel (INCD), and the Institutional Security Cabinet of the Presidency of the Republic of Brazil (GSI) are hereinafter referred to individually as a "Side" and jointly as the "Sides".

CONSIDERING that governments, businesses and consumers are increasingly faced with a variety of cyber threats and there is a need to further improve computer security readiness and raise awareness around the importance of keeping systems secure, and security practices and procedures;

ACKNOWLEDGING the need to strengthen the resilience of national and sectorial information infrastructures and related technologies, regulation and human resources

RECOGNISING further the importance of joint efforts by the Sides on cyber security; and

DESIRING to strengthen consistent and comprehensive cooperation between both Sides;

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

**ARTICLE 1**  
**Basic Principles**

1. The purpose of this MOU is to enhance the cooperation and the potential exchange of information between both Sides pertaining to Cyber Security.
  
2. This MOU
  - (a) Is not intended to create, maintain or govern any legally binding obligations, rights or benefits between the Sides or between the Sides and any third party; and
  - (b) Will be implemented subject to and in accordance with the Sides' domestic laws, regulations, policies and international obligations.
  
3. The Sides acknowledge that this MoU does not prejudice any existing or future arrangement or treaty relating to information disclosure, or other arrangement whether or not made under or with respect to the domestic law of the Sides.

**ARTICLE 2**  
**Scope of Co-operation**

The scope of co-operation between the Sides shall include areas that the Sides may mutually agree upon, such as exchange of information, human resources, capacity building and exchange of views regarding strategy and cyber security policy for the purposes of this MOU.

**ARTICLE 3**  
**Implementation**

The cooperation contemplated by this MOU may include the following activities and programs:

- (a) Detecting possible cyber security incidents (e.g. Denial of Service attacks, Phishing, serious scan attacks, and forgery/defacement of government websites);
  
- (b) Supporting each other in taking appropriate measures in order to prevent recurrence of such cyber security incidents;
  
- (c) Exchanging assessments of the prevailing cyber-security trend, as observed by each organisation, periodically;

- (d) Organizing visits of officials of two Sides as necessary to discuss current issues on cyber security;
- (e) Inviting each other to seminars/conferences held in respective countries to discuss cyber security issues;
- (f) Exploring opportunities for joint research and development on cyber security technologies;
- (g) Exchanging contact information (email, phone and fax numbers) and secure communication system with suitable publicly available encryption for exchanging sensitive information on cyber threats and vulnerabilities;
- (h) Exploring the possibility of conducting joint security drills;
- (i) Promoting and developing cooperation in the field of Education, Training and Capacity Building; and
- (j) Any other areas of Cooperation within the sides' respective authorities as may be mutually agreed upon.

#### **ARTICLE 4** **Point of contact**

1. For the purpose of identifying and facilitating programmes under Article 3, both Sides shall designate one or more representatives to maintain contact with the other. On behalf of the INCD, the Strategy and international cooperation division will serve as the point of contact for that matter. On behalf of the GSI, the Department of Information Security will serve as the point of contact. Each side may replace its designated Point of contact by informing the other side by a written notice.

2. The designated point of contact shall be responsible for defining the scope of co-operation as set out in Article 2 above.

#### **ARTICLE 5** **Ways of Co-operation**

1. All cooperative activities under Articles 2, 3 and 4 of this Memorandum of Understanding will be conducted in accordance with the applicable laws, rules, regulations and procedures of each country.

2. All cooperative activities under Articles 2, 3 and 4 of MoU will be subject to the availability of funds and other resources of Both Sides.



**ARTICLE 6**  
**Release of Information**

1. Neither Side shall 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.
  
2. Where national security, classified or operationally sensitive information is to be disclosed, the Side providing the information is responsible for ensuring 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.
  
3. Each Side will respect any condition, restrictions or caveat indicated by the other Side in respect of the handling or disclosure of information.
  
4. Each Side will keep the classification protocol and Traffic Light Protocol (TLP) of the shared information.

**ARTICLE 7**  
**Modifications**

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

**ARTICLE 8**  
**Disputes Settlement**

Any and all disputes between the Sides concerning the interpretation and/or implementation of this Memorandum of Understanding shall be settled amicably through consultations and/or negotiations between the Sides.

**ARTICLE 9**  
**Validity**

1. This Memorandum of Understanding will come into effect on the date of its last signature by the sides and shall remain in effect for a period of five (5) years unless terminated by either Side giving three (3) months' notice in writing to the other Side.
  
2. This Memorandum of Understanding may be renewed by mutual written consent of the Sides.

3. The termination of this Memorandum of Understanding shall not affect co-operative activities under Articles 2 and 3 or such separate agreements that are already in progress and until its completion, unless the Sides mutually agreed in writing otherwise.

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

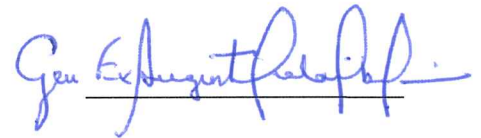
Signed in Jerusalem, Israel, on March 31<sup>st</sup>, 2019, in English. All communication between the Sides will be in English.

Which corresponds to the 24<sup>th</sup> day of Adar II 5779 in the Hebrew calendar, in the English language.

SIGNED for and on behalf of the  
Institutional Security Cabinet of the  
Presidency of the Republic of Brazil

**Augusto Heleno Ribeiro Pereira**

Minister of State head of the Institutional  
Security Cabinet of the Presidency of the  
Republic of Brazil



signature

31.3.2019

date

SIGNED for and on behalf of the Israel  
National Cyber Directorate

**Yigal Unna**

Director General



signature

31.3.19

date