MEMORANDUM OF UNDERSTANDING BETWEEN

THE FOREIGN COMMONWEALTH AND DEVELOPMENT OFFICE OF THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND

AND

THE INSTITUTIONAL SECURITY CABINET OF THE PRESIDENCY OF THE REPUBLIC OF BRAZIL

ON COOPERATION IN THE AREA OF CYBERSECURITY

The Foreign Commonwealth and Development Office of the United Kingdom of Great Britain and Northern Ireland and the Institutional Security Cabinet (*Gabinete de Segurança Institucional*) of the Presidency of the Federative Republic of Brazil are referred hereinafter individually as a "Participant" and jointly as the "Participants";

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

Recognising that the pace and development of new technologies and applications, in conjunction with greater access, offer significant opportunities for both economic and social development, the reliance on increasingly interconnected networks also exposes states to new vulnerabilities bringing profound impact on societies' well-being;

Given that the local networks even more interconnected by the internet bring a deep impact on the social well-being, but also expose the States to new vulnerabilities;

Reaffirming our commitment to promote an open, secure, stable, accessible, peaceful and interoperable cyberspace environment founded on respect to human rights and fundamental freedoms, where social and economic development can thrive;

Recognising that the threat of cyber criminality requires more effort to improve the security of the products and to promote cooperation among all stakeholders, within and across national borders, further the importance of joint efforts by the Participants on cyber security;

Desiring to develop the cooperation between the Participants in the area of Cyber Security, consistent with their respective domestic laws, rules and national regulations, their international obligations and based on equality, reciprocity and mutual benefit.

Acknowledging the importance of expanding bilateral cooperation to the field of cyber security as one of the most important aspects of maintaining international and national security aimed at preventing activities that intentionally and substantially damage the general availability or integrity of the Internet;

Have reached the following understanding:

ARTICLE 1
Basic Principles

The Participants hereby confirm their intention, under this Memorandum of Understanding (MoU), to promote closer and privileged cooperation and the exchange of information pertaining to cyber security, creating a wide-ranging partnership that reflects the shared values, democratic traditions, human rights, rule of law, national security and economic development of the Participants.

This MoU does not create, maintain or govern any legally binding obligations, rights or benefits between the Participants or between the Participants and any third party.

This MoU will be implemented subject to and in accordance with domestic laws, regulations, policies and international obligations of the Participants.

The Participants are committed to promote security and stability in cyberspace recognizing the applicability of international law, in particular the United Nations Charter, to responsible conduct of states in cyberspace, and the promotion of voluntary norms of responsible state behaviour in cyberspace.

The Participants understand the need to work closely with the private sector and business partners, mainly those considered critical infrastructures, acknowledging that much of the innovation and investment that shapes cyberspace takes place from within the private companies and that the multiple dimensions of the cyber security require cooperation between governments and their respective private sectors.

ARTICLE 2
Scope of Cooperation

The scope of cooperation between the Participants may include areas relating to Cyber Security that the Participants may mutually decide upon, such as the following:

a) Exchange experiences in regulation and views regarding national strategies, policies and best practices on cyber security;

b) Reviewing and exchanging experiences on legislation with a view to improving bilateral and international legal cooperation by promoting a closer cooperation among public agencies to combat cybercrime between the Participants;
c) Promoting measures in order to facilitate the exchange of information on cybercrimes in accordance with the respective national legislations;
d) Promoting cooperation between public agencies to combat cyber malicious acts and threats, including through training workshops, enhancing dialogue and processes, especially on digital forensics and legal frameworks, and setting up consultations as needed;
e) Improving the capacity of public agencies through equipping them to draft appropriate requests for electronic evidence in accordance with the respective laws and regulations;
f) Engaging in contact between the relevant governmental computer security incident response teams regarding active cyber incidents affecting the UK and Brazil using FIRST.org contact points.
g) Sharing best practices on the assessment, development and implementation of cyber security standards and certification provisions, and by strengthening the security of digital processes, products and services, throughout their lifecycle and supply chain;
h) Promoting cooperation in the fields of education, awareness, training, capacity building and exchange of knowledge between experts;
i) Considering opportunities to coordinate efforts for research and development for improved cyber security, and fostering academic interaction;
j) Establishing institutional mechanism for periodic exchange of views on outstanding issues pertaining to cyber incidents and current threats;
k) Discussing and sharing strategies to promote the integrity of the supply chain to enhance confidence of the users in the security of ICT products and services;

ARTICLE 3
Implementation

In order to implement the scope of cooperation identified in Article 2, the Participants will seek to develop the following programme:

(a) Identify opportunities to discuss cyber security incidents of mutual interest (e.g. Denial of Service attacks, Phishing, serious scan attacks, and forgery/defacement of government websites);
(b) Support each other in taking appropriate measures in order to prevent recurrence of such cyber security incidents and to bolster their efforts to increase threat information sharing;
(c) Exchange assessments of the prevailing IT security trend, as observed by each country, periodically;
(d) Organise visits of officials from both Participants to discuss current issues on cyber security. Continue to hold regular bilateral cyber discussions;

(e) Invite each other, as well as representatives from the private sector, academia and civil society, to seminars/conferences held in respective countries to discuss cyber security issues;
(f) Any other areas of cooperation regarding cyber security as may be mutually decided upon.

ARTICLE 4
Point of Contact

1. For the purpose of identifying and facilitating programs under Article 3, the Participants will designate representatives to maintain contact with each other. The designated points of contact will be responsible for seeking any required approval for the conduct of specific cooperative activities from their respective Governments.

2. The representatives from the Participants responsible for implementing the scope of cooperation, as set out in Article 2 above, 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 agreement, the Participants may hold working meetings alternately in Brazil and the United Kingdom at a mutually agreed date.

3. The designated representatives for the United Kingdom of Great Britain and Northern Ireland will be the Deputy Head of Mission of the United Kingdom to the Republic of Brazil and the Foreign, Commonwealth and Development Office's Cyber Lead for South America.

4. The designated representatives for the Republic of Brazil will be the designated Minister-Counselor of the Embassy of the Republic of Brazil to the United Kingdom and the Director of the Information Security Department of the Institutional Security Cabinet of the Presidency of the Republic of Brazil.

ARTICLE 5
Ways of Cooperation

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

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 the Participants.

3. To execute the activities of cooperation established in this MoU, invited guests from the private sector, security response teams, civil society and academia may be allowed to participate, if mutually decided by the Participants.

ARTICLE 6
Intellectual Property Rights

1. Each Participant will ensure appropriate protection of Intellectual Property Rights (hereinafter referred to as IPR) generated from cooperation pursuant to this MoU consistent with their respective laws, rules regulations and international agreements to which both Participants are committed.

2. The Participants will not assign any rights and obligations arising out of the IPR generated to inventions or activities carried out under this MoU to any third-party without consent of the other Participant.

ARTICLE 7
Release of Information

Neither Participant 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 Participant.

ARTICLE 8
Dispute Settlement

Any and all disputes between the Participants concerning the interpretation and/or implementation of this MoU will be settled amicably through consultations and/or negotiations between the Participants.

ARTICLE 9
Entry into Effect, Duration, Termination and Amendments

1. This MoU will come into effect immediately following the signature of both Participants.

2. The present MoU will remain in effect for an indefinite period of time.

3. This MoU may be amended by mutual written consent of the Participants, which will be formalised through diplomatic channels. The coming into effect of the amendments to the present MoU will be subject to the same procedure as for the coming into effect of the MoU.

4. The termination of this MoU will not affect cooperative activities under Articles 2 and 3 which are already in progress and until its completion, unless the Participants mutually determine in writing otherwise.

The undersigned, being duly authorised by their respective Participants, have signed this Memorandum of Understanding.

The foregoing record represents the understandings reached between the Foreign Commonwealth and Development Office of the United Kingdom of Great Britain and Northern Ireland and the Institutional Security Cabinet of the Presidency of the Republic of Brazil upon the matters referred to therein.

Signed in London, UK on this 21st day of November, 2022, in two originals each in Portuguese and English languages, both texts being equally authentic. In case of any divergence in interpretation, English text shall prevail.

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

Antonio Carlos de Oliveira Freitas
Special Advisor for Information Security at the Institutional Security Cabinet of the Presidency of the Republic of Brazil

signature

21 NOVEMBER 2022

date

SIGNED for and on behalf of the Foreign, Commonwealth & Development Office of the United Kingdom of Great Britain and Northern Ireland

William Middleton
Head of Cyber Policy Department at the Foreign, Commonwealth & Development Office of the United Kingdom of Great Britain and Northern Ireland

signature

21 November 2022

date