

MEMORANDUM OF COOPERATION
IN THE FIELD OF CYBERSECURITY
BETWEEN
THE INSTITUTIONAL SECURITY CABINET OF THE PRESIDENCY OF
THE FEDERATIVE REPUBLIC OF BRAZIL
AND
THE MINISTRY OF FOREIGN AFFAIRS OF JAPAN

The Institutional Security Cabinet of the Presidency of the Federative Republic of Brazil and the Ministry of Foreign Affairs of Japan (hereinafter collectively referred to as “the Participants” and individually as a “Participant”);

ACKNOWLEDGING the importance of cyberspace and its positive impact on the economic and social development of both countries, as well as the increasing use by both countries of information and communication technologies (ICT), networks, information systems and related technology, integrated to the Internet global network;

CONSIDERING that the threats to cybersecurity can endanger national security, critical infrastructure including information and communication systems, economic development and welfare of people;

CONVINCED that the Participants’ common purpose is to promote a free, open, secure, reliable and resilient cyberspace which fosters innovation and can be used as a tool for economic and social development of both countries and the promotion of human rights;

RESOLVED TO expand and strengthen bilateral cooperation between the Federative Republic of Brazil and Japan, promoting relevant joint initiatives in the field of cyberspace and cybersecurity, including exchange of good practices and information, development and implementation of domestic strategies and capacities, responses to cyberspace incidents, exchange of personnel, joint education and training, among others.

HAVE REACHED THE COMMON RECOGNITION AS FOLLOWS:

ONE

Objectives

This Memorandum is aimed at promoting cooperation on cybersecurity matters, which are a common interest of the Participants.

TWO

Working Group on Cyberspace and Cybersecurity

To accomplish the objectives mentioned in ONE above, the Participants may organize a Working Group on cybersecurity matters on an as-needed basis.

The Working Group may have the following functions:

- (a) To exchange views on political and strategic policies and organize cooperation between the Participants;
- (b) To establish a work plan on cooperation under this Memorandum;

- (c) To analyze and discuss the current and future global, regional, multilateral and bilateral policies on cybersecurity;
- (d) To identify and propose specific cooperation measures;
- (e) To facilitate and supervise cooperation under this Memorandum, as well as initiatives to be established by the Participants;
- (f) To encourage representatives from the private sector, civil society and academic world to participate in cooperation under this Memorandum; and
- (g) Other activities to be mutually decided by the Participants within the framework of this Memorandum.

The Working Group will be presided by such authorities as may be determined by the Participants and will hold meetings in person or by videoconference, as frequently as decided by the Participants.

THREE

Cooperation

To further promote the objectives mentioned in ONE above, the Participants may develop cooperation initiatives and actions in the following areas:

- (a) To promote joint work in international agencies and fora on cybersecurity matters by supporting and actively participating in initiatives and collaborating in line with positions of the Participants;
- (b) To make efforts to identify common positions and collaborate in actions at the regional and global level;
- (c) To promote and strengthen work and cooperation to combat cybercrime;

- (d) To develop measures to enhance cyberspace confidence and reliability, at global, regional and bilateral levels;
- (e) To foster the establishment of channels for exchange of information, detection and response;
- (f) To make efforts to promote cooperation in the development of cybersecurity policies and strategies;
- (g) To promote and develop cooperation in education, training, upskilling and improving capacities;
- (h) To foster dissemination activities on cybersecurity;
- (i) To share best practices on the assessment, development, and implementation of cybersecurity standards and regulations, and on the strengthening of the security of digital processes, products and services throughout their lifecycle and supply chain; and
- (j) To share best practices and regulations that could enhance the security of 5G network of both countries, which is becoming even more important as a fundamental social infrastructure.

FOUR

Cooperation methods and forms

Cooperation under this Memorandum may be conducted in the following ways:

- (a) Exchanging information, except for those marked as confidential, according to both countries' relevant laws and regulations on the protection of personal data and confidentiality of information;
- (b) Promoting training, education and upskilling programs;
- (c) Promoting cooperation and providing information between CSIRTs or CERTs of each Participant. For this Memorandum, CSIRTs means Computer Security Incident Response Teams, and CERTs means Computer Emergency Response Teams;

- (d) Using appropriate channels mainly focused on the exchange of information on cybersecurity threats and incidents affecting critical infrastructure and/or resources of both countries;
- (e) Participating in technical cooperation and training programs on cybersecurity matters and protection of critical infrastructure as well as research, conferences and other activities on the matter;
- (f) Exchanging publications, papers and academic material in case of similar threats to cybersecurity having affected or threatened to affect any agency in either country;
- (g) Exchanging information to prevent, mitigate or neutralize threats that may be originated in either country against assets located in each country, no matter whether they are public or private;
- (h) Fostering political and technical collaboration in multilateral instances connected with cybersecurity matters;
- (i) Making efforts to promote exchange of students, professors and technical staff, internships, research and development activities in the fields of cybersecurity;
- (j) Ensuring appropriate protection of intellectual property rights consistent with their respective laws, rules, regulations and international agreements to which both Participants are committed; and
- (k) Cooperating in other areas, to be determined on cybersecurity.

FIVE

Release of Information

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

SIX

Financial Considerations

Implementation of cooperation under this Memorandum will be subject to the availability of financial and human resources by each Participant.

Expenses to be incurred to conduct cooperation under this Memorandum will be conditioned upon the annual availability of funds by the Participants, according to both countries' respective laws and regulations.

SEVEN

Nature of this Memorandum

The Participants confirm that this Memorandum is not legally binding and does not give rise to rights or obligations under international law; it is a political and technical intention of the Participants to explore mutual cooperation ways on the matter, observing the national laws and regulations in the area of information security of each Participant.

EIGHT

Modification

Any modification to be made as a result of development or implementation of this Memorandum will be decided by mutual consent of the Participants in writing.

NINE

Settlement of disputes

Any dispute arising out of the implementation and/or interpretation of this Memorandum will be settled by the Participants through consultations with their best efforts on the basis of good faith.

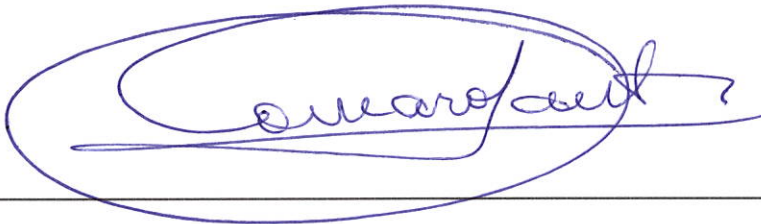
TEN

Commencement, duration and its discontinuation

This Memorandum will commence on the date of signing. Either Participant may discontinue this Memorandum at any time, by sending a written notice to the other Participant at least six (6) months in advance.

Discontinuation of this Memorandum will not affect any ongoing projects and initiatives under this Memorandum, unless otherwise mutually decided by the Participants.

Signed at the city of Brasilia/DF, Federal Republic of Brazil, on this 3rd day of May, 2024, in two originals each in Portuguese and English languages, both texts being equally valid. In case of any divergence in interpretation, English text will prevail.



Marcos Antonio Amaro dos Santos

MINISTER OF STATE HEAD OF THE INSTITUTIONAL SECURITY CABINET OF
THE PRESIDENCY OF THE FEDERATIVE REPUBLIC OF BRAZIL
FOR THE INSTITUTIONAL SECURITY CABINET OF THE PRESIDENCY OF
THE FEDERATIVE REPUBLIC OF BRAZIL



HAYASHI Teiji

AMBASSADOR EXTRAORDINARY AND PLENIPOTENTIARY OF JAPAN TO
THE FEDERATIVE REPUBLIC OF BRAZIL
FOR THE MINISTRY OF FOREIGN AFFAIRS OF JAPAN