



**MEMORANDUM OF UNDERSTANDING  
BETWEEN  
THE GOVERNMENT OF THE REPUBLIC OF INDONESIA  
AND  
THE GOVERNMENT OF AUSTRALIA  
ON CYBER COOPERATION**

The Government of the Republic of Indonesia, and the Government of Australia, (hereinafter referred to collectively as “the Participants” and singularly as “the Participant”);

**Noting** their shared interest in strengthening cooperation between Participants based on the principles of equality and reciprocity and thereby contributing to the mutual benefit and friendly relations between the two countries;

**Desiring** to promote open, free, secure, and peaceful use of cyberspace, which drives economic growth, protects national security and promotes international stability;

**Recognising** as a result of increasing interconnectivity, information systems and networks are now exposed to a growing number of threats and vulnerabilities which impact on both prosperity and national security;

**Reaffirming** their commitment to promote stability for cyberspace based on existing international law, voluntary and non-binding norms of responsible behaviour, practical confidence building measures, and cooperative capacity building;

**Recalling** and reaffirming commitments within the Joint Statement at the 2018 Australia - Indonesia Cyber Policy Dialogue, to act in accordance with voluntary non-binding norms of responsible behaviour; and

**Pursuant** to the relevant laws and regulations and international commitments of the Participants;

**Have reached** the following understandings:

## **Paragraph 1**

### **Purpose**

The purpose of this Memorandum of Understanding (hereinafter referred to as "MoU") is to promote partnerships and provide a framework of cooperation on cyber issues between the Participants.

## **Paragraph 2**

### **Areas of Cooperation**

The Participants will undertake to cooperate in the following areas:

#### **1) Sharing of Information and Best Practice**

- a. Participants will conduct information sharing on laws and legislation, national cyber strategies and policies, as well as cyber incident management procedures;
- b. Participants will consult and coordinate on cyber incident response and cyber threat information, especially when cyber incidents have a direct impact on the Participants;
- c. Participants will share views, experiences, lesson learned and best practices on cyber issues.

#### **2) Capacity Building and Strengthening Connection**

- a. Participants will support skills and knowledge development in cyber security and cyber policy through short-term training programs and long term awards (including scholarships for masters and PhD programs);
- b. Participants will facilitate links between institutions working in the field of cyber security including government, business or private sector and academia;
- c. Participants will explore linking research institutions and universities to strengthen teaching and research outcomes in cyber affairs;
- d. Participants will explore opportunities to promote international law, norms and responsible behaviours in cyberspace.

#### **3) Digital Economy**

- a. Participants will support business-to-business connections and growth of digital economy and innovation;
- b. Participants will support sharing of national policies, best practice and strategies to promote the digital economy.

#### **4) Cybercrime**

- a. Participants will promote stronger cyber forensic and investigation capabilities, including through sharing of training opportunities.



**Paragraph 3**  
**Cyber Policy Dialogue**

- 1) The Participants will conduct annual Cyber Policy Dialogues.
- 2) The dialogue has the purpose to advance the shared interests of the Participants related to the full spectrum of cyber issues, as well as a forum to exchange views and review their cooperation under this MoU.
- 3) Representatives from cyber related institutions of the Participants will participate in the dialogue.
- 4) The dialogue will be co-chaired by the Participants and be convened annually, or in any other time as mutually determined by the Participants.
- 5) The Participants will consult each other on the agenda of the dialogue, and the mutually determined agenda will be communicated through diplomatic channels, including the date and place of the dialogue.

**Paragraph 4**  
**Focal Points**

The Participants have identified the following focal points for the purpose of the implementation of this MoU:

- 1) For Indonesia: National Cyber and Crypto Agency (BSSN)
- 2) For Australia: Department of Foreign Affairs and Trade (DFAT)

**Paragraph 5**  
**Implementing Arrangements**

- 1) Institutions of the Participants may arrange between themselves the establishment of implementing arrangements, or other mutually determined written arrangements, in the field of cyber cooperation under this MoU.
- 2) The arrangements mutually determined upon by the institutions of the Participants will serve to implement the areas of cooperation.
- 3) The establishment, finalisation, and implementation of the arrangements under this MoU will be coordinated and by consent of the respective focal points as stipulated in Paragraph 4 of this MoU.

**Paragraph 6**  
**Financial Arrangements**

- 1) The Participants will bear its own costs associated with the activities and participation under this MoU.

- 2) Other financial arrangements may be carried out as mutually determined by the Participants.

**Paragraph 7**  
**Settlement of Dispute**

- 1) Any dispute arising out of the interpretation and implementation of this MoU will be settled amicably by the Participants through mutual consultations and negotiations between the Participants through diplomatic channels.
- 2) Disputes will not be referred to any third party, court or international tribunal.

**Paragraph 8**  
**Confidentiality**

- 1) The Participants commit to protect the confidentiality of information, technology, and/or data exchanged between the Participants under this MoU against unauthorized disclosure in accordance with the Participants domestic laws, regulations, policies, and directives. This does not apply where the information is legally accessible to the public.
- 2) Information, technology, and/or data exchanged under this MoU shall not be transmitted to a third party without prior written consent of the other Participants.
- 3) In the event of the expiration or termination of this MoU, provisions under this Paragraph shall still apply in terms of the confidentiality of this MoU.

**Paragraph 9**  
**Amendment**

The Participants may propose an amendment to this MoU by submitting it in writing to the other Participant. An amendment will be effected only upon the mutual written consent of the Participants.

**Paragraph 10**  
**Legal status of the MoU**

- 1) This MoU does not create any legally binding obligations, and does not alter or effect any existing agreements between the Participants.
- 2) The Participants acknowledge that this MoU is not an international agreement and will not create legal obligations governed by their respective domestic law or international law.



- 3) The terms of this MOU operate subject to, and do not supersede respective international obligations and domestic laws, policies and procedures of the participants.

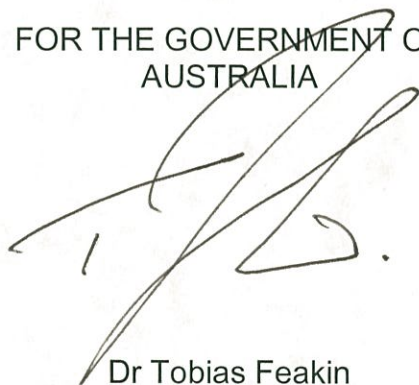
### Paragraph 11

#### Entry Into Effect, Duration, and Termination

- 1) This MoU will come into effect on the date of signature by both Participants and will remain in effect for a period of two (2) years, unless terminated by either Participants giving at least one (1) month prior written notice of the intended date of termination to the other Participant.
- 2) Termination of this MoU will not affect the implementation of activities that were decided upon or any ongoing activities prior to the date of termination.
- 3) This MoU may be extended at any time within the period it remains in effect by mutual written consent of the Participants.
- 4) Any intent to terminate or extend this MoU will be communicated through diplomatic channels.

SIGNED at Bogor on 31 August 2018, in two original copies in English and Indonesian languages, all texts being equally valid. In case of any discrepancy in interpretation, the English text will prevail.

FOR THE GOVERNMENT OF  
AUSTRALIA



Dr Tobias Feakin  
Ambassador for Cyber Affairs  
Department of Foreign Affairs and Trade  
of the Government of Australia

FOR THE GOVERNMENT OF THE  
REPUBLIC OF INDONESIA



Dr Djoko Setiadi, M.Si  
Head of National Cyber and Crypto  
Agency of the Republic of Indonesia