Concept Paper (Revised March 2019)

Australia-Malaysia

ASEAN Regional Forum (ARF) Points of Contact Directory on Security of and in the Use of Information and Communications Technologies (ICTs)

Purpose

The purpose of this project is to develop an ARF Directory to assist in:

- reducing tension and the risk of conflict arising from the misunderstanding and misperception of ICT security incidents, which could lead to miscalculation and possible escalation; and
- facilitating near real time communication in the event of ICT security incidents of potential regional security significance.
- Sharing of information on cyber security incidents

Background

2. Work by the ASEAN Regional Forum to date on ICT security confidence building measures has highlighted the importance of members knowing whom to contact in their own country and in other countries to address concerns about ICT security incidents and manage and respond to such incidents.

3. As a practical measure to contribute to improving connectivity and communication between ARF Participants, Australia and Malaysia are putting forward a proposal for an ARF Points of Contact Directory in relation to security of and in the use of ICTs of regional security significance (the Directory). This builds on the Australia-Malaysia ARF Workshop on Cyber Confidence Building Measures, held in Kuala Lumpur on 25-26 March 2014 and subsequent, related workshops. The concept is reflected in the ARF Work Plan on Security of and in the Use of Information and Communications Technologies adopted by the 22nd ASEAN Regional Forum in Kuala Lumpur on 6 August 2015.

Description

4. The Directory will consist of relevant points of contact from all participating ARF members, reflecting their unique domestic circumstances. Participation will be voluntary and the Directory will be available to participating ARF members only. The Directory will be validated, updated and recirculated at each iteration of the ARF Open Ended Study Group on Confidence Building Measures to Reduce the Risk of Conflict Stemming from the Use of ICTs (ARF Study Group), to ensure the contacts listed in the Directory remain current. The template of the proposed Directory is attached at Annex A.

Scope

5. The Directory is intended for the ARF and its membership. If an ARF Participant has a central agency or body nominated by their government to coordinate the nation's conflict prevention, crisis management and response in relation to security of and in the use of ICTs, a point of contact should be established within this body to serve as single point of contact for all ICT security incidents of regional significance.

6. For ARF Participants who do not have a single coordination point of contact nominated by their government, the channels detailed below can be used. Given its purpose, covering both prevention and response, the Directory may hold entries for:

- Diplomatic: Agencies responsible for promoting regional and international cooperation as well as conflict prevention on security of and in the use of ICTs. An example of such an agency could be the Ministry of Foreign Affairs.

- National Security and Policy Coordination: Ministries and agencies responsible for coordinating the nation's conflict prevention, crisis management and response in relation to security of and in the use of ICTs. Examples of such agencies could include Prime Minister's Department, Ministry of Interior, Ministry of Home Affairs, and Ministry of Communications.

- Enforcement: Law Enforcement authorities responsible for exchanging information as well as responding to and managing ICTs related crime. An example of such authorities would be Federal / National Police.
- Technical: Technical bodies or agencies responsible for exchanging ICT threat and vulnerability information as well as responding to and managing ICT security incidents. This could include National Cyber Security Agencies, Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs).

7. Governments organise themselves differently. It will be important to identify senior and working level contacts according to the above functions rather than by organisation or agency. It will also be important that contacts listed in the Directory understand how their national systems operate in term of identifying, managing, responding and mitigating ICT security incidents of potential national security concern. Each country's input to the Directory will be unique, and reflect their domestic circumstances. Some countries may list multiple agencies under one function, others may only list one for each function, while others may provide one single coordination point of contact. If a country prefers communications to be initiated through a particular channel or organisation, this should be noted in its entry to the Directory (at Annex A).

8. This Directory is not intended to produce a comprehensive listing of each government's ICT security officials, nor is it intended to identify hierarchies or lead agencies. The Directory is intended for the list of major contacts to be relevant in order to exchange information on ICT security incidents in the context of national, regional and international security.

9. Direct contact with *senior level officials* will occur only in times of potential regional security significance, which should be agreed by countries concerned. For ICT security incidents outside of such circumstances, communication should only occur between *working level contacts*. Senior level officials may only be contacted by other identified senior level officials. If senior

level counterparts are unavailable, senior officials may contact working level officials in relation to ICT security crises.

10. Contact details will include both telephone numbers and email addresses of senior and working level contacts. Countries can provide either or both, depending on capabilities as well as availability of staff. Senior officials can provide direct telephone numbers or provide the number of an aide or assistant. Entries will indicate whether contacts are available 24/7 or within business hours and languages spoken. Alternate contacts can be provided for outside of business hours if applicable. Technical points of contact may provide additional contact information for exchanging information.

Processes and Procedures

11. As set out in the 2015 ARF Work Plan on Security of and in the Use of ICTs, additional policies and procedures for sharing information between ARF contact points on preventing ICT crises as well as criminal and terrorist use of ICTs, will be developed, if needed, via the ARF Study Group, which submit recommendations to the ARF Inter-Sessional Meeting on Security of and in the Use of ICTs (ARF ISM on ICTs Security)., for approval by ARF Ministerial Meeting via the ARF Inter-sessional Support Group on Confidence Building Measures and Preventive Diplomacy (ARF ISG on CBMs and PD) as well as the ARF Senior Officials Meeting (ARF SOM). Initial policies and procedures are provided in Annex B.

12. Each country will determine their respective point of contact for each specific ICT security incident, taking into account the technical details and possible consequences. Any information exchanged will be voluntary and in line with the respective domestic circumstances of the ARF Participants involved. ARF Participants involved in the information exchange will only share that information with third parties by mutual consent. ARF Participants should keep a record of all information exchanged.

13. The decision on how to respond to communications received via the Directory and the content to be communicated will be determined by each country. Any subsequent cooperation and/or information sharing will proceed according to mutual agreement.

Existing Directories

14. There are existing directories which provide some of the material that will be covered by the ARF Directory. However, no existing Directory has the same scope as the proposed ARF Directory. The existing Directories include but are not limited to:

- International Critical Information Infrastructure Protection Directory (the Meridian Directory)
- The G8 24/7 Network on High Tech Crime
- Asia Pacific CERT Points of Contact
- ASEAN Regional Forum Ministry of Foreign Affairs Points of Contact.

15. In case the contact points of this Directory overlap with other existing directories for ICT security incidents, countries concerned will discuss and decide the processes and procedures to be applied based on mutual consent.

[*Pilot Program*

**. We welcome nominations to participate in the Directory for consideration and discussion at the next ARF Study Group meeting and subsequent ARF ISM on ICTs Security*. (Delete this para, if this CBM is agreed)]

Future Work

16. The ARF Open Ended Study Group will develop, if needed, additional policies and procedures for sharing information between ARF contact points on preventing ICT crises as well as criminal and terrorist use of ICTs and will submit recommendations to the ARF ISM on ICTs Security, for approval by ARF Ministerial Meeting via the ARF ISG on CBMs and PD as well as the ARF SOM.

Annex A

ARF ICT Security Point of Contact Directory

Country X

Function	Department/Agency	Senior level contact	Working level contact
Single Coordination Point of Contact *Countries that have a single point of contact may choose to provide these details only.*	XXXX	Name: Title/Position: Email: Phone: Languages: Availability: [24 hr / business hours]	Name: Title/Position: Email: Phone: Languages: Availability: [24 hr / business hours]

AND/OR

Function	Department/Agency	Senior level contact	Working level contact
Diplomatic *Agencies responsible for promoting regional and international cooperation as well as conflict prevention on ICTs security. An example of such an agency could be the Ministry of Foreign Affairs.*	XXXX	Name: Title/Position: Email: Phone: Languages: Availability: [24 hr / business hours]	Name: Title/Position: Email: Phone: Languages: Availability: [24 hr / business hours]

Function	Department/Agency	Senior level contact	Working level contact
National Security and Policy Coordination *Ministries and agencies responsible for coordinating the nation's conflict prevention, crisis management and response in relation to security of and in the use of ICTs. Examples of such agencies could include Prime Minister's Department, Ministry of Interior, Ministry of Home Affairs, and Ministry of Communications.*	XXXX	Name: Title/Position: Email: Phone: Languages: Availability: [24 hr / business hours]	Name: Title/Position: Email: Phone: Languages: Availability: [24 hr / business hours]
Enforcement *Law Enforcement authorities responsible for exchanging information as well as responding to and managing the ICTs related crime. An example of such authorities would be Federal / National Police.*	XXXX	Name: Title/Position: Email: Phone: Languages: Availability: [24 hr / business hours]	Name: Title/Position: Email: Phone: Languages: Availability: [24 hr / business hours]

Function	Department/Agency	Senior level contact	Working level contact
Technical *National ICT Security Agencies and/or National Computer Emergency Response Teams (CERTs) and/or Computer Security Incident Response Teams (CSIRTs)Technical bodies or agencies responsible for exchanging ICT threat and vulnerability information as well as responding to and managing ICT security incidents. This could include National Cyber Security Agencies, Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs).*	XXXX	Name: Title/Position: Email: Phone: Languages: Availability: [24 hr / business hours] Additional Information: [for example, websites, encryption key, etc.]	Name: Title/Position: Email: Phone: Languages: Availability: [24 hr / business hours] Additional Information: [for example, websites, encryption key, etc.]

Annex B

Procedure for Inquiry

ARF participants may use the following steps to request information from another participant regarding an ICT security incident:

1. Call or email the relevant point of contact and provide your name and affiliation.
2. Provide as much information as possible regarding the nature of the incident.
3. Ask for additional information about the incident and provide your contact information. Indicate time sensitivity as appropriate.
4. Nominate preferred channel of communication and nominate the agency within your country that will become the primary point of contact for this specific incident.

Procedure for Responding to an Inquiry

ARF participants may follow these steps to respond to an inquiry about an ICT security incident:

1. Provide an immediate response to the ICT security incident query (if possible), or:
2. Inform the point of contact that you will look into the ICT security incident and follow up with additional information. Provide an estimated timeframe for a response, as appropriate; and
3. Agree on preferred channel of communication and nominate the agency within your country that will become the primary point of contact for this specific incident.