~ KEYNOTE SPEECH - OIC-CERT: PAST, PRESENT AND FUTURE ~

HIS EXCELLENCY GENERAL TAN SRI DATO' SERI PANGLIMA MOHD AZUMI BIN MOHAMED (RETIRED)

CHAIRMAN OF THE BOARD OF DIRECTORS,

CYBERSECURITY MALAYSIA

ORGANISATION OF ISLAMIC COOPERATION – COMPUTER EMERGENCY RESPONSE TEAM (OIC-CERT)

ANNUAL CONFERENCE 2016

14TH DECEMBER 2016 (WEDNESDAY) || 10.25 A.M.

OIC HEADQUARTERS, JEDDAH, KINGDOM OF SAUDI ARABIA

Salutations

1. **His Excellency Dr. Yusuf bin Ahmad al-Othaimeen**
   Secretary General, Organisation of Islamic Cooperation (OIC)

2. **His Excellency Engineer Badar Ali Said Al Salehi**
   Chair, Organisation of Islamic Cooperation – Computer Emergency Response Team / Director General, Oman National CERT (OCERT)

3. **His Excellency Dr. Ewan Ward**
   Chair, Asia Pacific Computer Emergency Response Team (APCERT)

4. **His Excellency Mr Wajdi Alquliti,**
   Director of IT Department, Organisation of Islamic Cooperation (OIC)
5. **Distinguished Participants**

6. **Ladies and Gentlemen.**

1. السَّلاَمُ عَلَيْكُمْ وَرَحْمَةُ اللهِ وَبَرَكَااتُه

2. بِسْمِ ٱللَّهِ ٱلرَّحْمَـنِ ٱلرَّحِيم

3. Let me begin by congratulating His Excellency Dr Yusof bin Ahmad Al Othaimeen as the Secretary General of The OIC. The appointment speaks for itself and with Your Excellency’s wisdom and guidance, Insyaallah The OIC, a global Islamic Organization, the second largest inter-governmental organization after The UN, will continue to propel to greater heights and achievements.

   It is indeed a great honour and privilege for me, being the former Chair of The OIC Cert and its current Advisor to the Chair, to be asked to deliver this keynote speech “OIC-CERT, PAST, PRESENT AND FUTURE” at this 2016 Annual Conference. I also wish to express my sincere gratitude to the OIC, the host for this year’s OIC-CERT AGM and Annual Conference, for the consistent and generous support provided to the OIC-CERT.

(*Mandate*)
Excellencies, Ladies and Gentlemen,

4. The idea of establishing a CERT among OIC countries began in 2005 with the conceptualisation of the **OIC-CERT Task Force** during the Conference of Knowledge and ICT for Development **2005** (KICT4D 2005) held in conjunction with the Annual Meeting of the Islamic Development Bank Board of Governors in Putrajaya, Malaysia. This was followed by the formation of the OIC-CERT Task Force in a meeting in Kuala Lumpur in 2006 where Malaysia was appointed as the Chair of the task force. In 2008 at the 35th session of the Council of Foreign Minister the OIC-CERT was formalised Foreign Ministers in Kampala, Uganda. Resolution reads “Encourage all member states to take the necessary measures, to encourage Their National CERT to collaborate with the OIC-CERT, which will be a grouping dedicated in providing support and responding to computer incidents”. Following this, The OIC-CERT had its 1st Annual General Meeting held in Kuala Lumpur, Malaysia, in January 2009 where the Steering Committee was established and members were appointed.

5. In **May 2009** the OIC-CERT became an **affiliated Institution of the OIC**. This was an important milestone for OIC-CERT as it re-enforced the recognition and trust of the OIC-CERT from the OIC.

6. In May 2010, the **37th Session of the Council of Foreign Ministers**, held in **Dushanbe, Republic of Tajikistan** reaffirmed is support for the **OIC-CERT** initiative. OIC-CERT was to invite Member States which are yet to join the OIC-CERT and to extend the necessary support for member states to strengthen confidence building of cooperation and trust for a peaceful, secured, resilient and open cyber environment. These are important steps taken for members to reach a common ground in how we respond to threats to international cyber security.

(*Vision and Objective*)
Excellencies, Ladies and Gentlemen,

7. The OIC-CERT was established with the **vision** to be a leading cyber security platform to make the cyber space safe. Through the provision of a platform to develop cyber security capabilities and promoting global collaboration.

8. The **objectives** of the OIC-CERT are as reflected:

a. strengthening the relationships amongst CERTs in the OIC Member Countries, OIC-CERT partners and other stakeholders in the OIC member domain;

b. encouraging experience and information sharing in cyber security;

c. preventing and reducing cyber-crimes, harmonizing cyber security policies, laws and regulations;

d. building cyber security capabilities and awareness amongst member countries;

e. promoting collaborative research, development and innovation in cyber security;

f. promoting international cooperation with international cyber security organizations; and *g.* assisting OIC-CERT member countries with the establishment and development of their national CERTs.

9. Following its inception, Alhamdulillah, with the consistent support of its members, AGMs and Annual Conference and technical trainings were carried out in Malaysia, Egypt, Morocco, Indonesia, UAE, Oman and this year in Saudi Arabia. These are lead some of the confidence building measures under taken by the OIC-CERT to strengthen the trust, enhance early warning their minimizing or preventing the escalation of the threat and its predictability and enhancing relations amongst the member states.

(*Membership*)
Excellencies, Ladies and Gentlemen,

10. Today, in a span of 7 years, the OIC-CERT has grown, from a modest 7 founding **members** in 2006, to 41 members from 21 OIC countries, spanning across the globe, from the Middle East to Africa and Asia.

11. The current membership from 21 countries represents only 37 percent of the total 57 OIC member states. It is important to note that if we look at the statistics provided by the Internet World Statistics, we will notice that the OIC internet users are approximately 611 million out of 3.5 billion internet users. This represents 19.5% of the world internet user, which is a substantial figure. Moving forward, such cooperative measures, collaborative and communication mechanisms will see OIC-CERT membership getting access to global networking that promotes strategic cooperation and new ventures with CERT communities or information security communities around the world, it will also provide an opportunity for resource and information sharing. Also membership in the OIC-CERT will offer assistance to members in establishing CERTs in technical expertise and policy advices. In this respect, much needs to be done.

12. We understand that it took the OIC forty years to grow from a humble beginning of a membership of 25 in 1970 to 57 members today. We hope that the OIC-CERT can do better, speed-wise and we plan to do so. Taking the cue from The APCERT which is now expanding itself into The Pacific Island

Nations. (Quote request from Iraq). In this regard, we hope that the OIC, through the leadership of His Excellency Dr. Yusuf bin Ahmad al-Othaimeen, will support and assist us.

13. We should not rely on The OIC to spearhead this. On its part, The OIC-CERT needs to scale up advocacy and promotion programs so as to attract more member states to join. We should not allow a repetition of the resolution at the 37th session of The Council Of Foreign Ministers in 2010.

(*Strategic Pillars*)

Excellencies, Ladies and Gentlemen,

14. Membership alone is not enough, much remains to be done. We need to preserve with other CERTs like The APCERT to reach a common ground or consensus on how we respond to international cyber security that requires extensive cooperation and consensus building for it to be credible. We need to assist OIC Member States to develop their capabilities. We need to be ready to face the series of cyber security challenges that has emerged. A holistic strategic program and achievable goals is needed to ensure OIC Member States readiness in facing today's challenges. The OIC-CERT has established **six strategic pillars** to support the strategic program. The strategic pillars are:

a. organisation structure;
b. international cooperation;
c. standard and regulation;
d. technical and technology,
e. capacity building; and
f. promotion and awareness.

Pursuant to this, we are embarking on various strategic initiatives.

(*Pillar 1: Organisation Structure*)

15. The first strategic pillar is Organisation Structure led by Oman, which deals with governance that steer the policy direction and ensure the implementation

of the strategic programs and facilitate the mechanism and interaction points by which the strategic program shall be implemented. The OIC-CERT Steering Committee is tasked with driving the policy direction through the six strategic pillars. To date, the 2016-2017 OIC-CERT business plan is already developed and its implementation is in progress.

(*Pillar 2 - International Cooperation*)

16. Realising that **international cooperation** and collaboration, is an important facet of cyber security, the OIC-CERT will continue to reach out with other organisations with similar aspirations. Hence, the International Cooperation and Promotion pillar led by Oman. We believe that, at the multi-lateral level, such as the APCERT, African CERT, ARF, needs to be strengthened continuously through collaborative and communication mechanisms. Some of which are already underway. Pursuant to this, in 2011, the OIC-CERT signed a Memorandum of Understanding (**MoU**) with the Asia-Pacific Computer Emergency Response Team (**APCERT**), in Dubai. Both parties agreed:

a. to exchange information about the current and future developments among the members of the two regional CERTs;

b. to have joint cyber exercises base on the mutual agreement of both parties;

c. to mutually appoint liaison members to act as the point of contact with regards to information exchange between the parties;

d. to dispatch, on a best effort basis, representatives to attend each other's seminars and conferences, to the extent that is deemed appropriate by both parties; and

e. to involve each other in projects that have relevant context base on mutual agreement of both parties.

(*International cooperation. Cooperation with APCERT. Joint conference 2015*)

17. This mutual understanding between the two organisations to foster closer collaboration in incident prevention and response, led to an inaugural joint

APCERT and OIC-CERT Annual Conference in Kuala Lumpur in 2015. This 5-day event attracted nearly 700 participants both local and international. We hoped that similar joint events will be organised in the future.

18. The OIC-CERT also signed an MoU with the International Information System Security Certification Consortium (ISC)^2 on May 19 this year.

19. At the moment, we are working on a Memorandum of Understanding with the Forum of Incident Response and Security Teams **(FIRST**), a leading global organisation in incident response and also with the International Telecommunication Union (**ITU**). Both MoUs are expected to be signed next year.

(*International Cooperation – OIC-CERT Portal*)

20. Another part of international collaboration is the establishment of smart platform for the OIC cyber security community to collaborate, network, share knowledge, and market products. This can be done through an **online portal**. Malaysia as the Permanent Secretariat of the OIC-CERT has embarked on an online portal development project. This portal is ready for use and was launched at our AGM last Sunday. We hope this platform can further enhance international collaboration among the OIC-CERT members.

(*Pillar 3: Standards and regulations*)

21. The **Standards and regulations** is about quality and minimum requirement for organisation to comply for information security. Egypt and Iran have taken this task to create and enhance a common set of standards, policies, procedures and regulations for OIC-CERT to address the issue of cyber security and cyber-crime. Both countries are working on databases of cyber security laws and regulations to be compiled at the OIC-CERT portal for reference, development of OIC-CERT cyber security standard operating policies, procedures and best practices and establishing an information dissemination protocol.

(*Pillar 4: Technical and technology*)

22. The **Technical and Technology Pillar** is about the know-how, of overcoming workforce constraints and limited resources faced by OIC-CERT members in mitigating cyber incidents. This is to develop and implement technical solutions and technologies to proactively address the issue of cyber threats among OIC-CERT members. Iran, as the led for Technical and Technology, is looking into the methodology for the sharing and enhancement of technical solutions and technologies among OIC-CERT members.

(*Pillar 5: Capacity Building*)

23. **Capacity building** led by Indonesia and Malaysia, is an important facet of cyber security where we need to address issues related to human capital development at various stages of education. Since its inception, the OIC-CERT has conducted various cyber security capacity building initiatives. These initiatives are: Training; Malware Research, Cyber Drills; and Professional Certification Program.

(*Capacity Building - Training*)

24. An integral part of capacity building program is training. CyberSecurity Malaysia organised a 10-day training course, fully sponsored by the Government of Malaysia, entitled “Effective Incident Management and Active Defence Training” for 15 participants from ASEAN and OIC-CERT member countries. This training was held under the Malaysian Technical Cooperation Programme (MTCP), on 1-10 August 2016, in Kuala Lumpur.

25. Indonesia, through the Indonesia Security Incident Response Team on Internet Infrastructure / Coordination Centre (IDSIRTII/CC), organised the OIC-CERT Digital Forensics Workshop, in Bali, Indonesia, on 28 Oct 2016.

26. The OIC-CERT will try to make these kind of trainings to be an annual event or a regular affair for the OIC-CERT.

(*Capacity Building - Cyber Drill*)

27. Another capacity building initiative is the **Cyber Drill** which is intended to provide an opportunity to face a realistic incident, testing out internal procedures, exercise technical capabilities and analyse cyber threats and to

identify the level of readiness to mitigate the emerging of cyber threats and to avoid serious impact to the country. This initiative was first conducted in 2012 with 5 teams from 5 OIC-CERT member countries and it was conducted annually ever since. In 2015 the participation increased to 13 teams from 11 countries. However, in 2016, only 6 teams from 6 countries participated. We need to strive to increase this number in 2017 and beyond. We will continue to organise the Cyber Drill in the future relevant to the current cyber security landscape and hope more members will participate.

(*Capacity Building - Malware Research*)

28. Another capacity building program is on malware research. One of the threats faced today is malware which is becoming increasingly sophisticated, intelligent, versatile, easily available, and is affecting a broader range of targets and devices. As such, Malaysia initiated a Malware Research and Coordination Facility for the OIC-CERT which was approved for implementation during the 7th OIC-CERT Annual General Meeting (AGM) in Kuala Lumpur, Malaysia. It is a research project that started in September 2015 that analyse malware data from member countries or organizations. Presently, six organisations from four countries participated in this project.

29. The objectives of this facility are to perform:

a. advanced cyber malware analytics;
b. research and coordination among the OIC countries; and
c. a holistic view of the threats and coordinate response among the OIC countries.

This facility will provide a Malware Repository for the OIC-CERT, and centralised malware advisories and analysis. The report or data can also be used as input to conduct impact analysis on economic development in participating organization or country. We hope more members will participate in this program in the very near future.

(*Capacity Building - Professional Certification*)

30. **Professional certification** is an important mechanism to build human capital in cyber security. We are considering the idea of a **OIC-CERT Global Accredited Cybersecurity Education (ACE) Scheme**. The objective is to create world class competent work-force in cyber security and promote the development of cyber security professional programmes within the region. It is expected that this initiative will provide cyber security professionals in OIC countries with the right knowledge, skills, abilities and experience. This is a new initiative and we hope it will come to fruition in the very near future.

(*Pillar 6: Awareness*)

31. Creating **awareness** is another important facet in cyber security. It is about the transformation process in cultivating best practices in every aspect of conducts which lead to safer cyber space towards creating resilient environment. To this effect, Nigeria is looking into promoting cyber security cooperation and coordination in mitigating of cyber incident. This pillar is still at the early stage of development. We hope that the awareness program will progress swiftly.

(*Conclusion*)
Your Excellency, Ladies and Gentlemen,

32. For the future, increased activities in the years ahead is to be expected if the OIC-CERT wants to remain relevant in the international system in response to existing or emerging challenges. In sum, it is building partnerships. Present day situation requires our thinking and actions to be multi focussed, multi layered and multi stakeholder through international collaboration, interconnected solutions. We need to push for a cyber security agenda amongst the members of the OIC. Our work will never be over. Cyber threats will be evolving and will be a constant threat to societies and countries. Our responsibility is to equip ourselves to be ever ready in facing these challenges. I would urge OIC member states to develop their cyber security capabilities and support the proposed strategic programs framework. At the same time, OIC-CERT will strive to be the implementation arm for the OIC cyber security initiatives as mandated. In its introduction to the “Realistic

Goals for the Promotion of peace in cyber space, the ICT4 Peace Foundation aptly remarked that “The world is currently facing another challenge that is here to stay: an invasive, multi pronged and multi layered threat, a modern day arms race without visible actors and attributable actors, characterized by an escalating number of attacks both on and off the radar”. Tackling such a threat requires, “a global effort, a concerted open dialogue to find common grounds and solutions”. The order for the day should be cyber cooperation and cyber diplomacy. There is a need for trust building and transparency. This calls for training, capacity building, development assistance, collaboration and cooperation. For the OIC-CERT and that of others. We need to reach to an agreement our wide range of measures and initiatives at building the bridges for cooperation towards a peaceful, secured, resilient, safe and transparent cyber environment. We must not, at all costs, allow our differences, be it ideological etc be the barrier or stumbling block to reaching agreement and consensus. On the norms and confidence building measures in responding to international cyber challenges.

33. With these few thoughts, I would like to reaffirm Malaysia’ commitment, as the Permanent Secretariat, to work closely with members to address the present and future challenges in cyber security.

34. On that note, I would like to thank once again for inviting me to speak at the 2016 Annual Conference.

35. May Allah grant us help and guidance.

/END/