MEDIA RELEASE

FOR IMMEDIATE RELEASE

GOVERNMENT LAUNCHES NATIONAL CYBER CRISIS MANAGEMENT POLICY AND MECHANISM

Policy to strengthen the national cyber defense readiness among the Critical National Information Infrastructure (CNII) agencies

KUALA LUMPUR (27 November 2013) – In addressing the emerging issue of cyber threat which poses serious challenges to the economic wellbeing and security of the nation, the National Security Council (NSC) has organised the National Cyber Crisis Exercise 2013 (X-MAYA 5). This annual event aims to test the effectiveness of the procedures that have been developed under the Malaysian National Cyber Crisis Management Plan and to assess the readiness and preparedness of critical national infrastructure agencies against cyber attacks. X-MAYA 5 2013 marks a significant milestone in the history of the event with the achievement of highest number of participations, 98 public and private agencies across the 10 Critical National Information Infrastructure – namely Health, Water, Banking and Finance, Information and Communications, Energy, Transport, Defense and Security, Government, Food and Agriculture and Emergency Services.

The Honourable Tan Sri Dato' Muhyiddin Bin Hj. Mohd Yassin, Deputy Prime Minister of Malaysia has officiated The Closing Ceremony of the National Cyber Crisis Exercise 2013 (X-MAYA 5) on 26 November 2013 at the Royale Bintang Damansara Hotel, Petaling Jaya, Selangor. The Deputy Prime Minister has also launched a national policy document, "National Security Council's Directive No. 24: Policy and Mechanism of the National Cyber Crisis Management". This executive directive outlines Malaysia's strategy for cyber crisis mitigation and response through public and private collaboration and coordination. The roles and responsibilities of all CNII agencies are clearly defined in this document. There are six (6) main principles under this directive namely National Cyber Crisis Management Structure; National Cyber Threat Level; Computer Emergency Response Team (CERT); Cyber Security Protection Mechanism; Response, Communication and Coordination procedure and Readiness Programme.

Over the time, the level of cyber preparedness among CNII sectors has improved as more organisations came to realize the importance of having a proper internal mechanism and procedure in managing cyber security incidents. During the drill, they were able to detect and respond to the attack in timely manner. In order to reduce the gap between agencies, the NSC will take the initiatives to facilitate those agencies so that they could further improve their cyber security response, communication and coordination procedure.

CyberSecurity Malaysia provided technical support and infrastructure for X-MAYA 5. "We leveraged our experience in organizing cyber drill for the Organisation of Islamic Cooperation - Computer Emergency Response Team (OIC-CERT) and the Asia Pacific Computer Emergency Response Team (APCERT) as well as in dealing with cyber security incidents through our Cyber999 Help Centre and Malware Research Centre," said Dr Amirudin Abdul Wahab, CyberSecurity Malaysia's Chief Executive Officer.

CyberSecurity Malaysia
(726630-U)
Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999
www.cybersecurity.my

Since Malaysia is progressing towards a developed digital economy by 2020 with the pervasive use of information and communication technology (ICT) in all aspects of the economy, it is vital to create a secured ecosystem within the cyber environment. X-MAYA provides a thorough evaluation of Malaysia's CNII agencies to strengthen national emergency response by ensuring that proper procedures and mechanisms are in place for effective monitoring of the CNII, incident reporting and response, communications dissemination and business continuity management.

~ The End ~

CyberSecurity Malaysia is the national specialist centre for cyber security, under the purview of the Ministry of Science, Technology and Innovation (MOSTI).

For additional information, please visit our website at http://www.cybersecurity.my. For general inquiry, please email to info@cybersecurity.my Stay connected with us on www.facebook.com/CyberSecurityMalaysia and www.twitter.com/cybersecuritymy

For further enquiries about this document, please call +603-89926888,
Mohd Shamil Mohd Yusoff (ext: 6978), email shamil@cybersecurity.my or
Sandra Isnaji (ext: 6977), email sandra@cybersecurity.my