MALAYSIA'S NATIONAL CYBER SECURITY POLICY

Towards an Integrated Approach for Cybersecurity and Critical Information Infrastructure Protection (CIIP)

2009 ITU Regional Cybersecurity Forum for Africa and Arab States
Tunis, Tunisia (4-5 June 2009)

MOHD SHAMIR B HASHIM
Strategic Policy & Cyber Media Research
CyberSecurity Malaysia
shamir@cybersecurity.my

THE BRAND LAUREATE
CyberSecurity Malaysia
Best in Corporate Branding
Internet Security

Securing Our Cyberspace

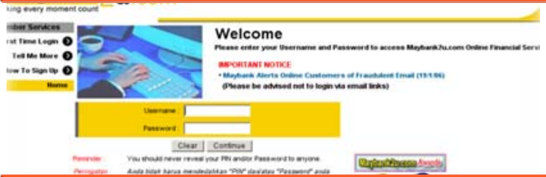
CYBER THREATS

CyberSecurity MALAYSIA

Technology Related Threats

Hack Threat

Fraud



…ing every moment count

…ber Services

…rst Time Login

Tell Me More

…ow To Sign Up

Home

Welcome

Please enter your Username and Password to access Maybank2u.com Online Financial Servi…

IMPORTANT NOTICE

- Maybank Alerts Online Customers of Fraudulent Email (19/1/06)

(Please be advised not to login via email links)

Username:

Password:

Clear | Continue

Reminder: You should never reveal your PIN and/or Password to anyone.

Peringatan: Anda tidak harus mendedahkan "PIN" dan/atau "Password" anda

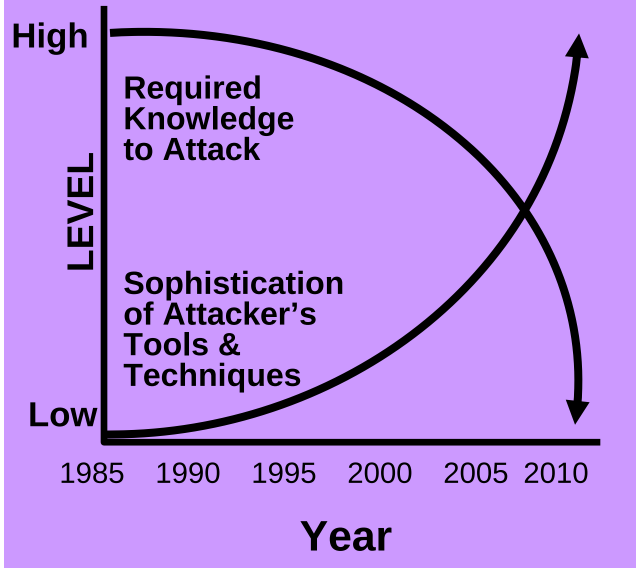
Malicious Code

Denial of Service Attack

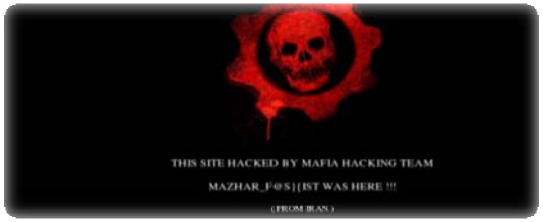
Harassment

Securing Our Cyberspace

Growing World-wide Cyber Threats



Intrusion



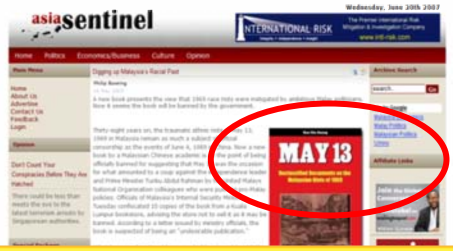
THIS SITE HACKED BY MAFIA HACKING TEAM

MAZHAR_F@S||IST WAS HERE !!!

(FROM IRAN)

Cyber Content Related Threats

National Security



Wednesday, June 20th 2007

asiasentinel

INTERNATIONAL RISK — The Premier International Risk Mitigation & Investigation Company — www.intl-risk.com

Home | Politics | Economics/Business | Culture | Opinion

Main Menu: Home, About Us, Advertise, Contact Us, Feedback, Login

Opinion

Don't Count Your Conspiracies Before They Are Hatched

There could be less than meets the eye to the latest terrorism arrests by Singaporean authorities.

Digging up Malaysia's Racial Past

Philip Bowring

A new book presents the view that 1969 race riots were instigated by ambitious Malay politicians. Now it seems the book will be banned by the government.

Thirty-eight years on, the traumatic ethnic riots of May 13, 1969 in Malaysia remain as much a subject of official censorship as the events of June 4, 1989 in China. Now a new book by a Malaysian Chinese academic is on the point of being officially banned for suggesting that May 13 was the occasion for what amounted to a coup against the independence leader and Prime Minister Tunku Abdul Rahman by United Malays National Organization colleagues who were pushing pro-Malay policies. Officials of Malaysia's Internal Security Ministry Tuesday confiscated 15 copies of the book from a Kuala Lumpur bookstore, advising the store not to sell it as it may be banned, according to a letter issued by ministry officials, the book is suspected of being an "undesirable publication."

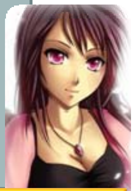
MAY 13 — Declassified Documents on the Malaysian Riots of 1969

Archive Search — search... Go

Affiliate Links

Sedition / Defamation

Online Porn



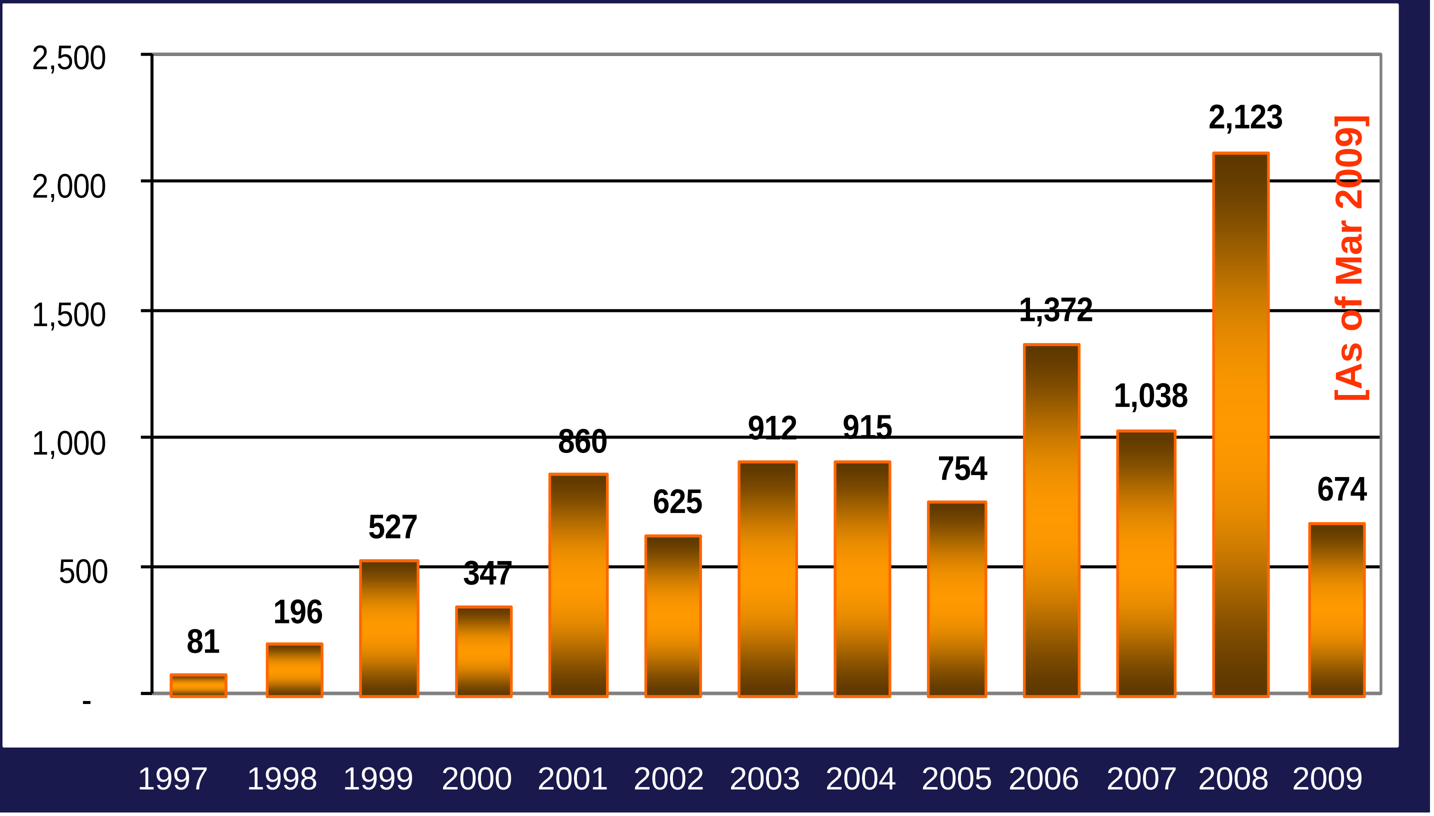
Hate Speech

CYBER SECURITY INCIDENTS
1997 - 2008

- A total of 10,424* security incidents referred since 1997
- For the Mar 2009, total no. of spams detected was a whopping 199,274

Type of incidents:

- Intrusion
- Destruction
- Denial-of-Service
- Virus
- Hack Threat
- Forgery
- Harassment



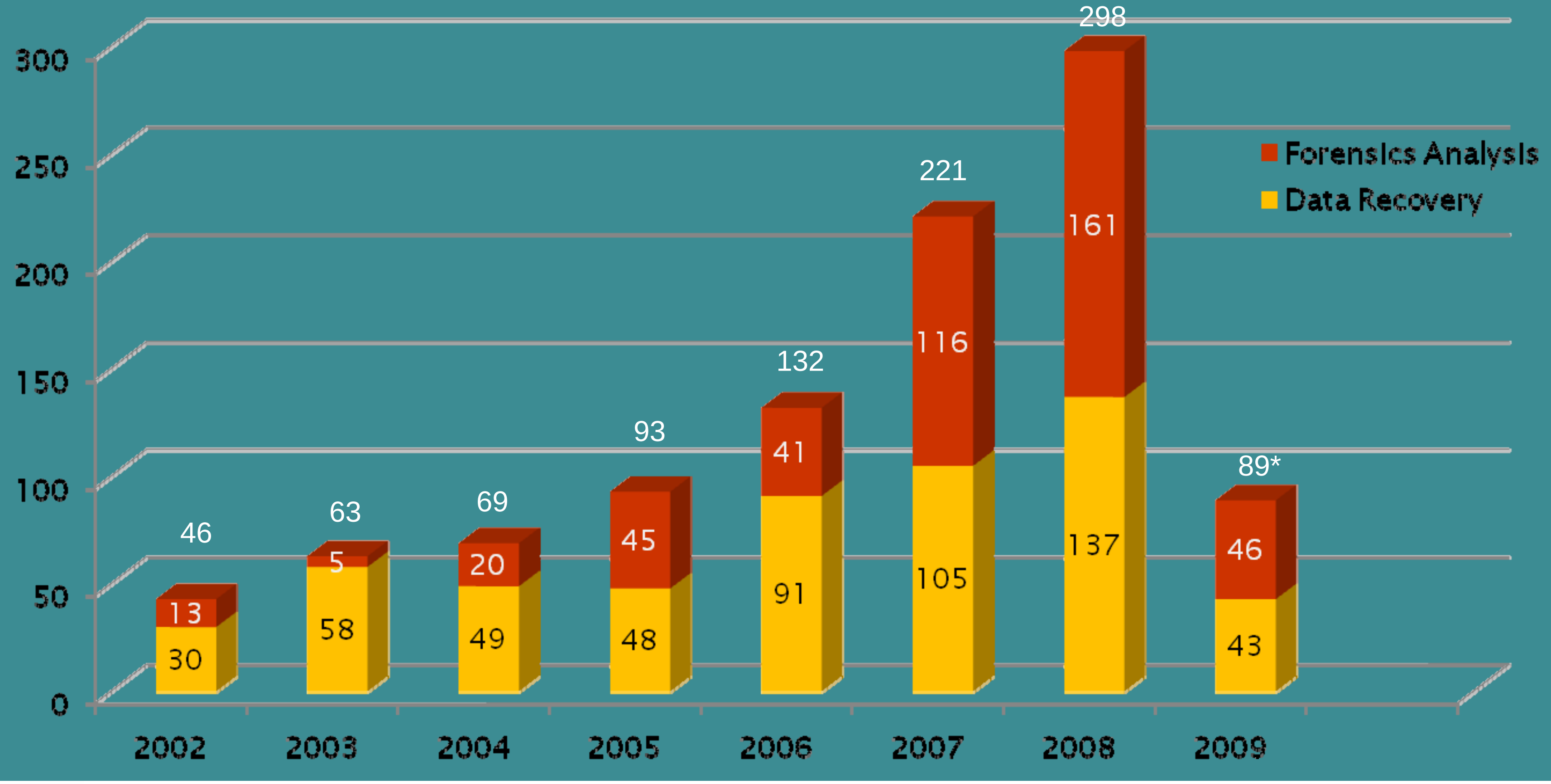
Securing Our Cyberspace

* As of Mar 2009 (excluding spams)

Number of cyber security incidents* referred to CyberSecurity Malaysia

DIGITAL FORENSICS CASES
2002 - 2009

- 75% cases - from law enforcement agencies (Police, Central Bank, Securities, etc).
- Types of cases – Financial Fraud, Sexual Assault, national threats, etc.



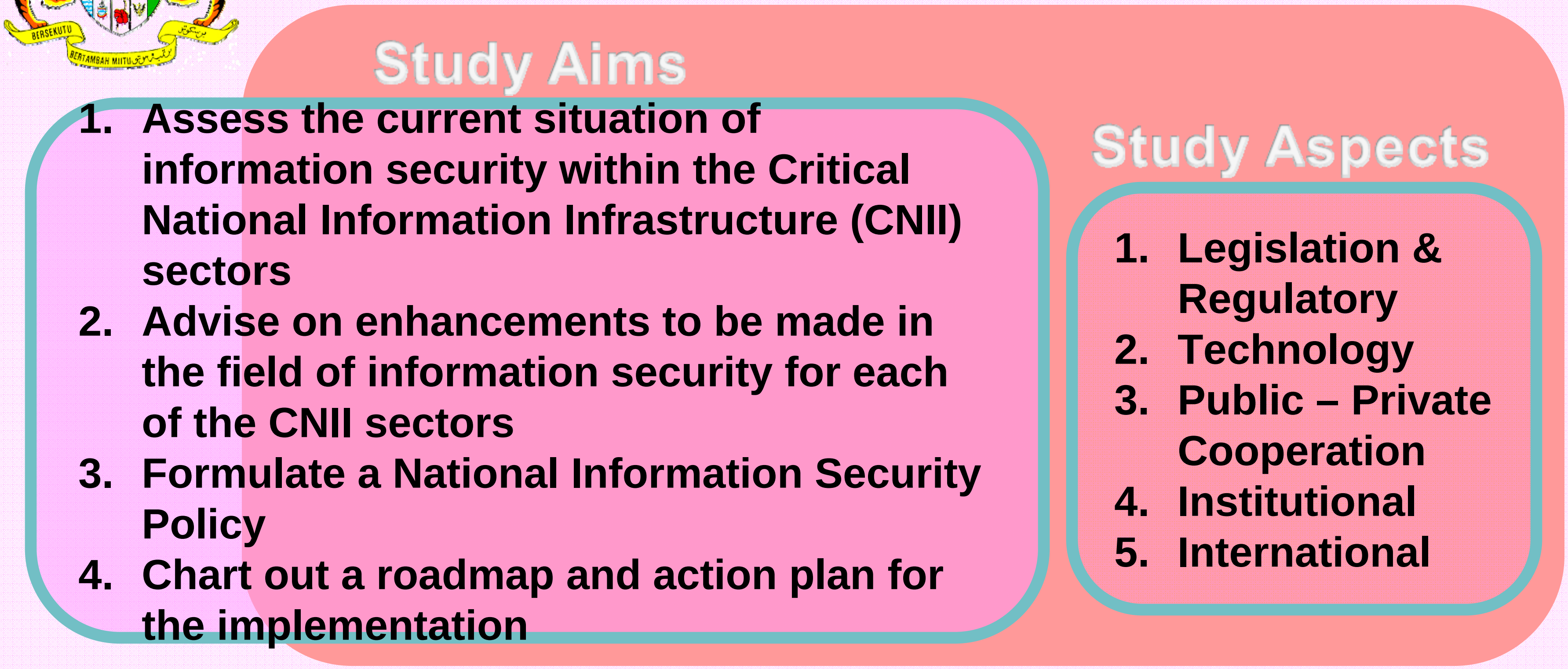
Securing Our Cyberspace

* As of Mar 2009

The STUDY
- National Information Security Policy

Ministry of Science, Technology and Innovation conduct study 2005 - 2006

Accepted by the Government 2006



Study Aims

1. Assess the current situation of information security within the Critical National Information Infrastructure (CNII) sectors
2. Advise on enhancements to be made in the field of information security for each of the CNII sectors
3. Formulate a National Information Security Policy
4. Chart out a roadmap and action plan for the implementation

Study Aspects

1. Legislation & Regulatory
2. Technology
3. Public – Private Cooperation
4. Institutional
5. International

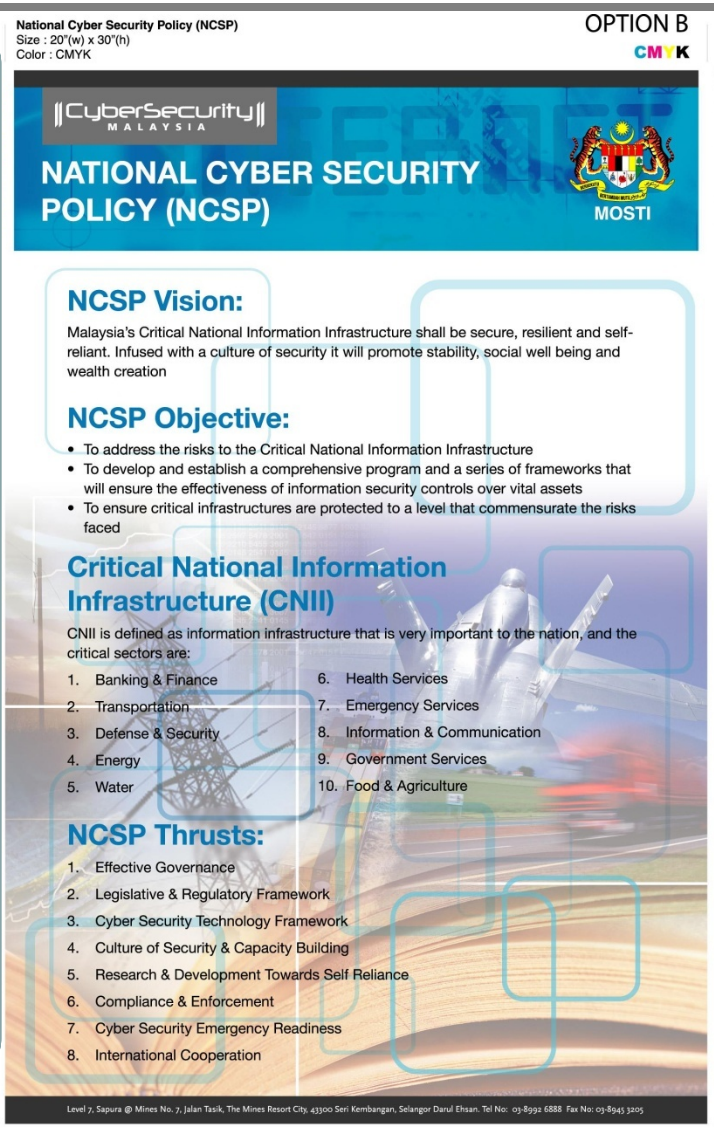
The NATIONAL CYBER SECURITY POLICY - Overview

OBJECTIVES

1 ADDRESS THE RISKS TO THE CRITICAL NATIONAL INFORMATION INFRASTRUCTURES

2 TO ENSURE THAT CRITICAL INFRASTRUCTURES ARE PROTECTED TO A LEVEL THAT COMMENSURATE THE RISKS FACED

The policy recognises the critical and highly interdependent nature of the CNII and aims to develop and establish a comprehensive programme and a series of frameworks that will ensure the effectiveness of cyber security controls over vital assets



National Cyber Security Policy (NCSP)
Size : 20"(w) x 30"(h)
Color : CMYK

OPTION B

CMYK

NATIONAL CYBER SECURITY POLICY (NCSP)

MOSTI

NCSP Vision:

Malaysia's Critical National Information Infrastructure shall be secure, resilient and self-reliant. Infused with a culture of security it will promote stability, social well being and wealth creation

NCSP Objective:

- To address the risks to the Critical National Information Infrastructure
- To develop and establish a comprehensive program and a series of frameworks that will ensure the effectiveness of information security controls over vital assets
- To ensure critical infrastructures are protected to a level that commensurate the risks faced

Critical National Information Infrastructure (CNII)

CNII is defined as information infrastructure that is very important to the nation, and the critical sectors are:

1. Banking & Finance
2. Transportation
3. Defense & Security
4. Energy
5. Water
6. Health Services
7. Emergency Services
8. Information & Communication
9. Government Services
10. Food & Agriculture

NCSP Thrusts:

1. Effective Governance
2. Legislative & Regulatory Framework
3. Cyber Security Technology Framework
4. Culture of Security & Capacity Building
5. Research & Development Towards Self Reliance
6. Compliance & Enforcement
7. Cyber Security Emergency Readiness
8. International Cooperation

Level 7, Sapura @ Mines No. 7, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan. Tel No: 03-8992 6888 Fax No: 03-8945 3205

CNII – Critical National Information Infrastructure

The NATIONAL CYBER SECURITY POLICY - Overview

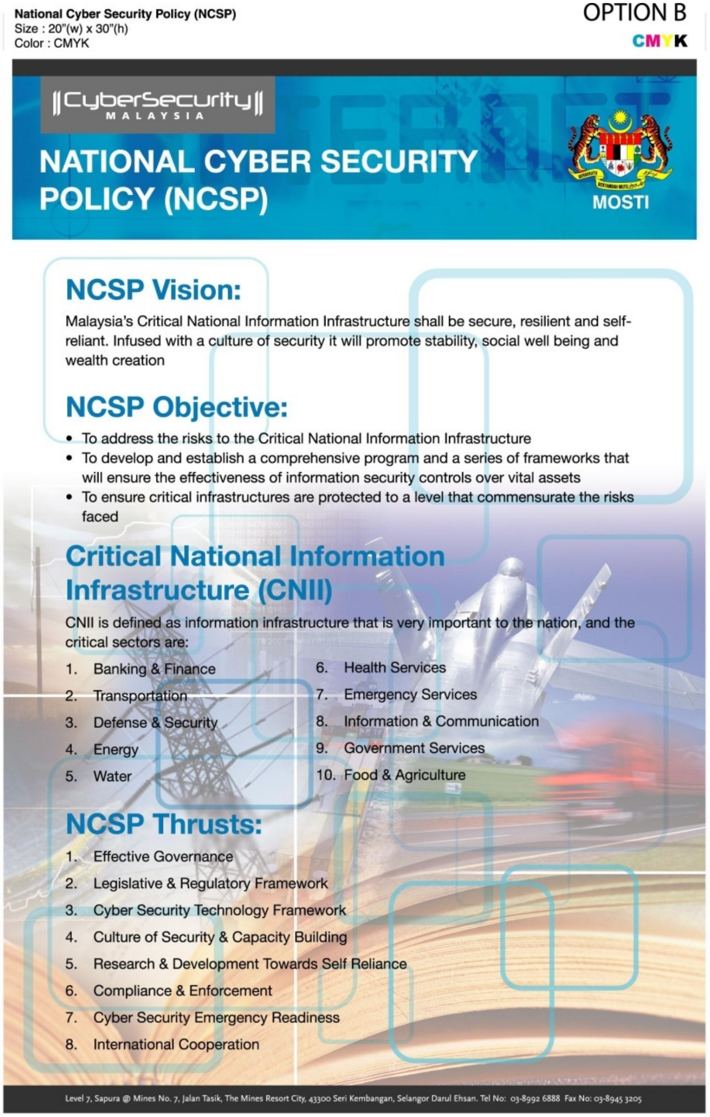
VISION

'Malaysia's Critical National Information Infrastructure shall be secure, resilient and self-reliant. Infused with a culture of security, it will promote stability, social well being and wealth creation'

CNII

Assets (real & virtual), systems and functions that are vital to the nation that their incapacity or destruction would have a devastating impact on

1. National economic strength
2. National image
3. National defense & security
4. Government capability to function
5. Public health & safety



National Cyber Security Policy (NCSP)
Size : 20"(w) x 30"(h)
Color : CMYK

OPTION B

CMYK

NATIONAL CYBER SECURITY POLICY (NCSP)

MOSTI

NCSP Vision:

Malaysia's Critical National Information Infrastructure shall be secure, resilient and self-reliant. Infused with a culture of security it will promote stability, social well being and wealth creation

NCSP Objective:

- To address the risks to the Critical National Information Infrastructure
- To develop and establish a comprehensive program and a series of frameworks that will ensure the effectiveness of information security controls over vital assets
- To ensure critical infrastructures are protected to a level that commensurate the risks faced

Critical National Information Infrastructure (CNII)

CNII is defined as information infrastructure that is very important to the nation, and the critical sectors are:

1. Banking & Finance
2. Transportation
3. Defense & Security
4. Energy
5. Water
6. Health Services
7. Emergency Services
8. Information & Communication
9. Government Services
10. Food & Agriculture

NCSP Thrusts:

1. Effective Governance
2. Legislative & Regulatory Framework
3. Cyber Security Technology Framework
4. Culture of Security & Capacity Building
5. Research & Development Towards Self Reliance
6. Compliance & Enforcement
7. Cyber Security Emergency Readiness
8. International Cooperation

Level 7, Sapura @ Mines No. 7, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan. Tel No: 03-8992 6888 Fax No: 03-8945 3205

Securing Our Cyberspace

The NATIONAL CYBER SECURITY POLICY
- CNII Sectors

DEFENCE & SECURITY

TRANSPORTATION

BANKING & FINANCE

HEALTH SERVICES

EMERGENCY SERVICES

ENERGY

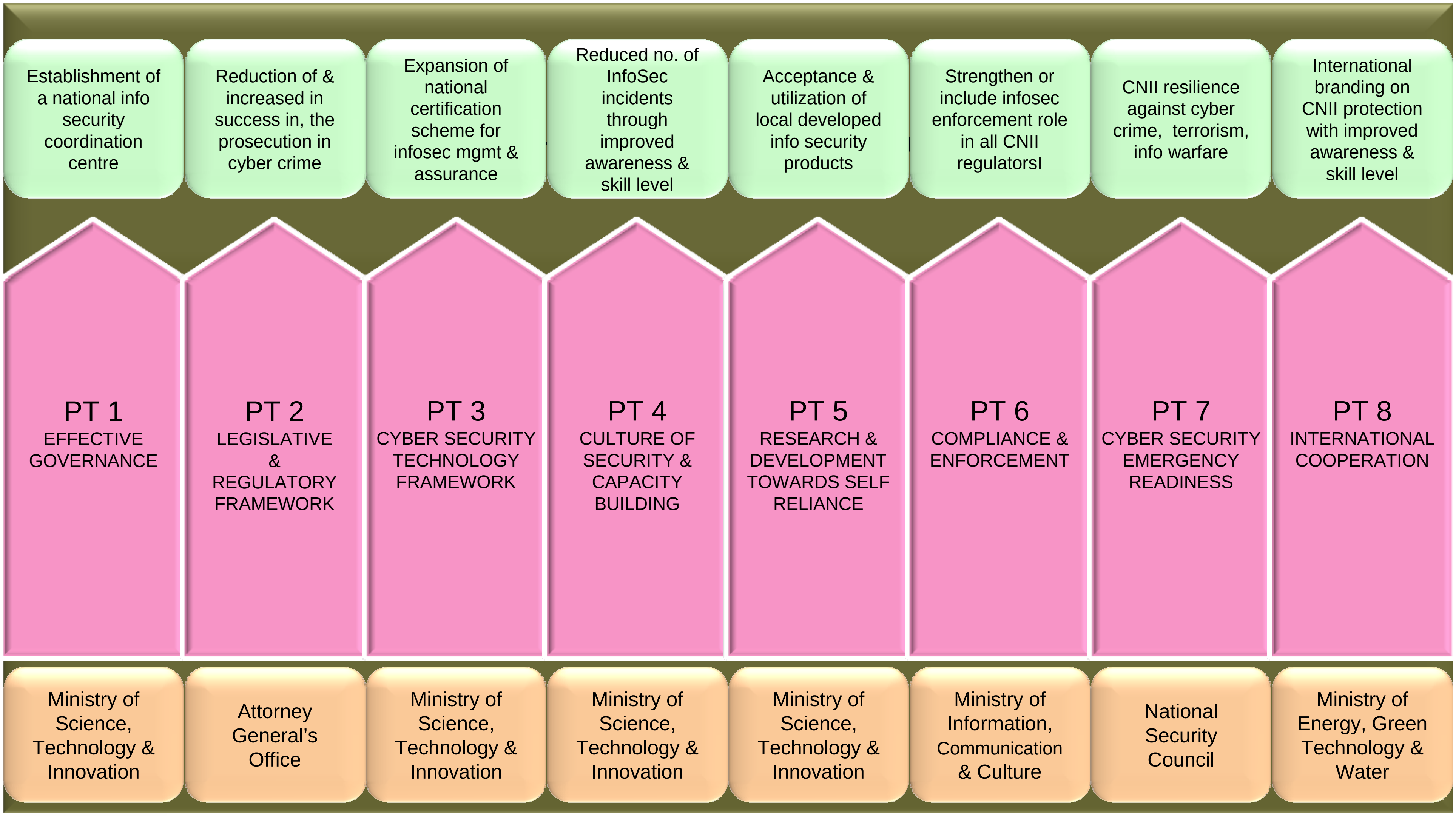
INFORMATION & COMMUNICATION

GOVERNMENT

FOOD & AGRICULTURE

WATER

The NATIONAL CYBER SECURITY POLICY - Policy Thrusts

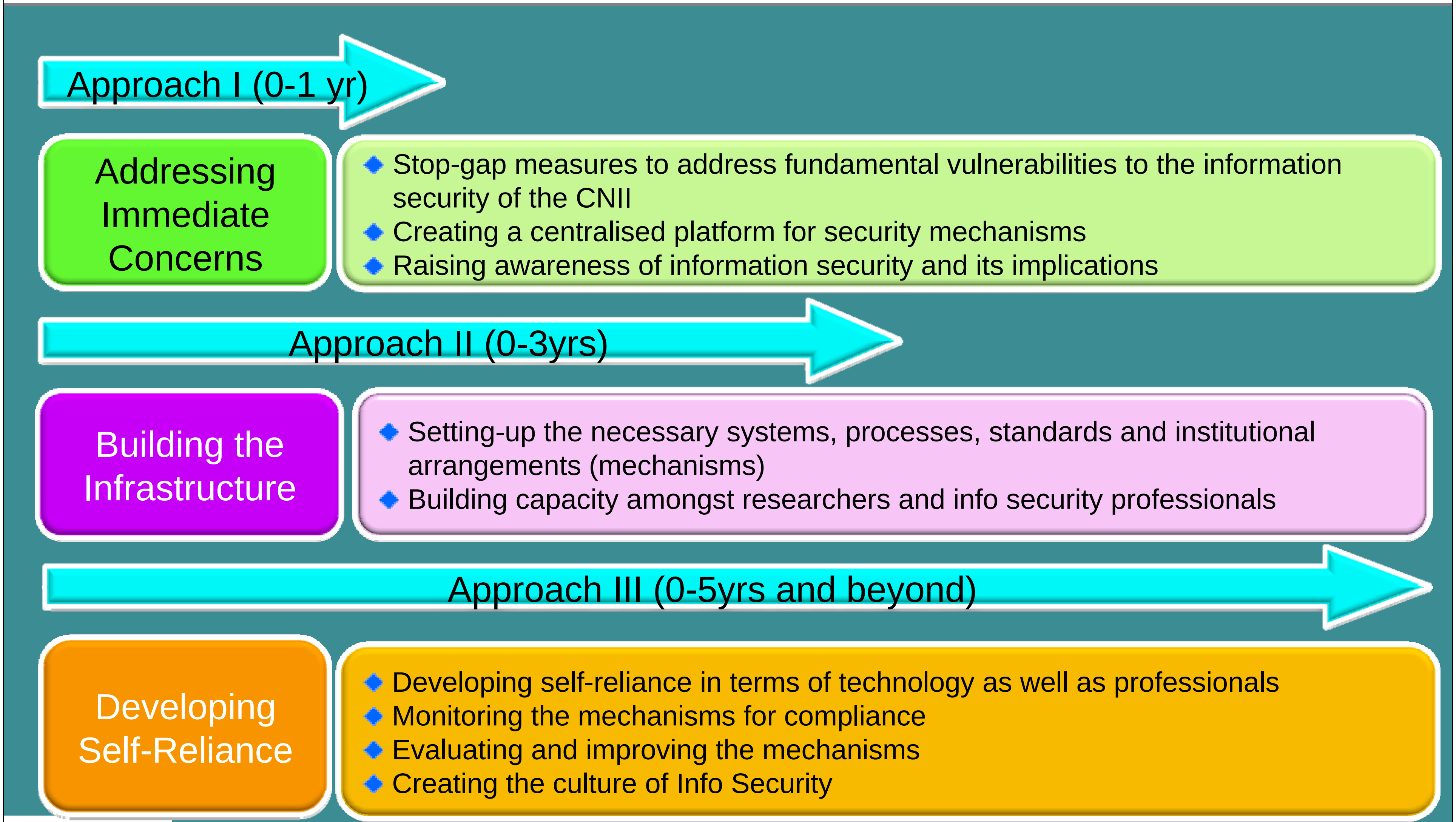


Establishment of a national info security coordination centre	Reduction of & increased in success in, the prosecution in cyber crime	Expansion of national certification scheme for infosec mgmt & assurance	Reduced no. of InfoSec incidents through improved awareness & skill level	Acceptance & utilization of local developed info security products	Strengthen or include infosec enforcement role in all CNII regulatorsI	CNII resilience against cyber crime, terrorism, info warfare	International branding on CNII protection with improved awareness & skill level
PT 1 EFFECTIVE GOVERNANCE	PT 2 LEGISLATIVE & REGULATORY FRAMEWORK	PT 3 CYBER SECURITY TECHNOLOGY FRAMEWORK	PT 4 CULTURE OF SECURITY & CAPACITY BUILDING	PT 5 RESEARCH & DEVELOPMENT TOWARDS SELF RELIANCE	PT 6 COMPLIANCE & ENFORCEMENT	PT 7 CYBER SECURITY EMERGENCY READINESS	PT 8 INTERNATIONAL COOPERATION
Ministry of Science, Technology & Innovation	Attorney General's Office	Ministry of Science, Technology & Innovation	Ministry of Science, Technology & Innovation	Ministry of Science, Technology & Innovation	Ministry of Information, Communication & Culture	National Security Council	Ministry of Energy, Green Technology & Water

PT – Policy Thrust

Securing Our Cyberspace

The NATIONAL CYBER SECURITY POLICY
- Implementation Approaches



Approach I (0-1 yr)

Addressing Immediate Concerns

- Stop-gap measures to address fundamental vulnerabilities to the information security of the CNII
- Creating a centralised platform for security mechanisms
- Raising awareness of information security and its implications

Approach II (0-3yrs)

Building the Infrastructure

- Setting-up the necessary systems, processes, standards and institutional arrangements (mechanisms)
- Building capacity amongst researchers and info security professionals

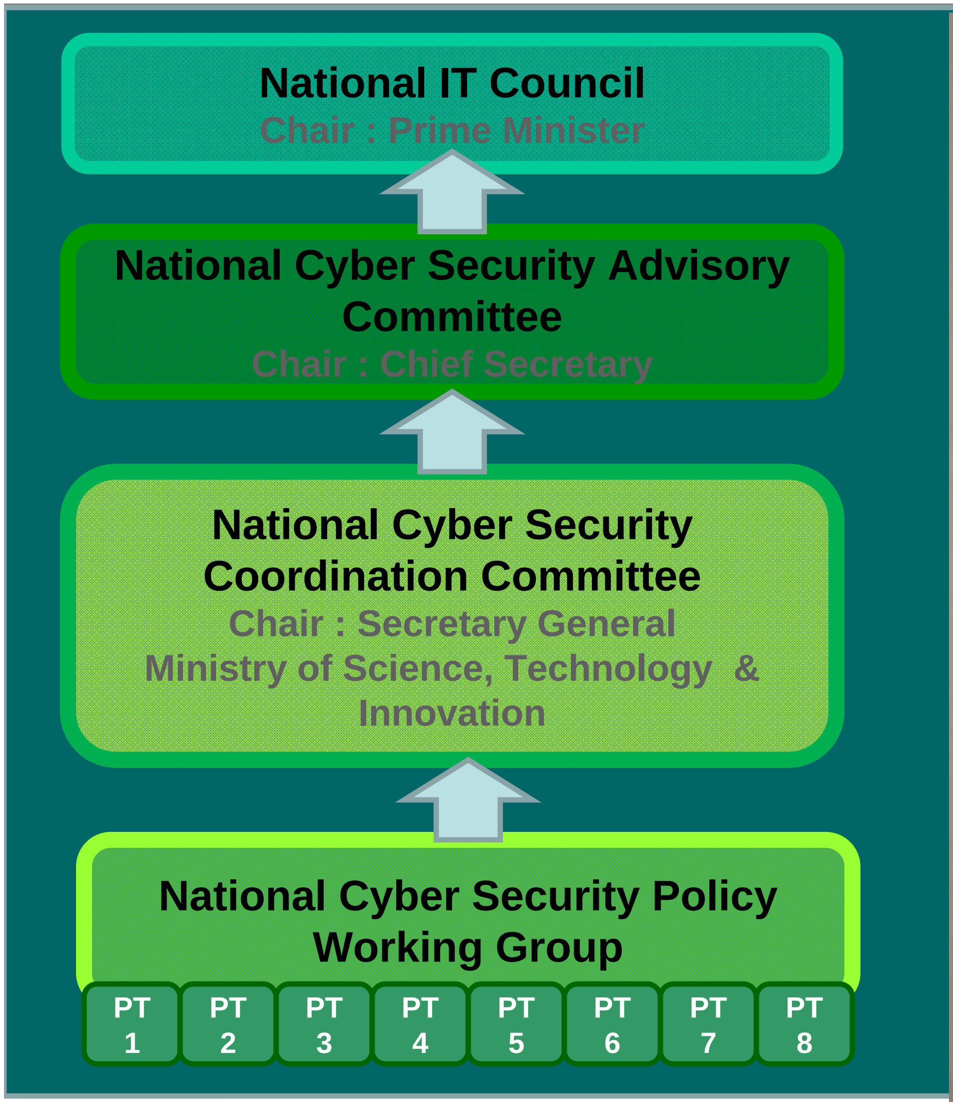
Approach III (0-5yrs and beyond)

Developing Self-Reliance

- Developing self-reliance in terms of technology as well as professionals
- Monitoring the mechanisms for compliance
- Evaluating and improving the mechanisms
- Creating the culture of Info Security

Securing Our Cyberspace

The NATIONAL CYBER SECURITY POLICY
- Effective Governance



National IT Council
Chair : Prime Minister

National Cyber Security Advisory Committee
Chair : Chief Secretary

National Cyber Security Coordination Committee
Chair : Secretary General
Ministry of Science, Technology & Innovation

National Cyber Security Policy Working Group

PT 1 | PT 2 | PT 3 | PT 4 | PT 5 | PT 6 | PT 7 | PT 8

1. Malaysian Administrative, Modernisation and Management Planning Unit
2. Attorney General's Chambers
3. Ministry of Science, Technology and Innovation
4. Ministry of Defence
5. Ministry of Foreign Affairs
6. Ministry of Energy, Green Technology and Water
7. Ministry of Information, Communications & Culture
8. Ministry of Finance
9. Ministry of Transport
10. Ministry of Home Affairs
11. National Security Council
12. Chief Government Security Officer's Office
13. Central Bank of Malaysia
14. National Water Services Commission
15. Malaysian Communications & Multimedia Commission
16. Energy Commission
17. Securities Commission
18. CyberSecurity Malaysia

Securing Our Cyberspace

The NATIONAL CYBER SECURITY POLICY
- Legislative & Regulatory Framework

A Study on the laws of Malaysia to accommodate legal challenges in the Cyber Environment

1) To identify the issues and challenges with regard to the Internet.

2) To address the current legislative framework, both cyber-specific and conventional and to assess if the current legislation is sufficient to address such menaces.

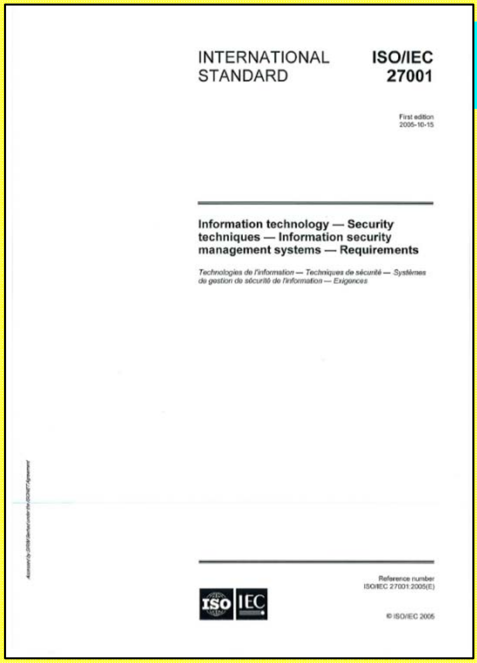
3) To make recommendations of the type of amendments required. This would also include addressing methods and processes of reconciling and harmonising the legislation where general comments will be made of the current legislation.

The NATIONAL CYBER SECURITY POLICY
- Cyber Security Technology Framework

To increase the robustness of the CNII sectors by complying to international standards:

MS ISO/IEC 27001:2006
Information Security Management System (ISMS)

The International Standards



INTERNATIONAL STANDARD

ISO/IEC 27001

First edition
2005-10-15

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2005(E)

© ISO/IEC 2005

Adopted as Malaysian Standards

MALAYSIAN STANDARD

MS ISO/IEC 27001:2006

INFORMATION TECHNOLOGY- SECURITY TECHNIQUES - INFORMATION SECURITY MANAGEMENT SYSTEMS - REQUIREMENTS
(ISO/IEC 27001:2005, IDT)

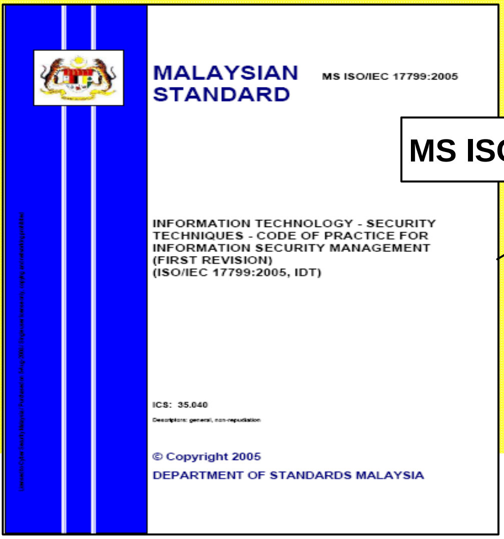
ICS: 35.040

Descriptors: ISMS, requirements

© Copyright 2006

DEPARTMENT OF STANDARDS MALAYSIA

MS ISO/IEC 27001:2006



MALAYSIAN STANDARD

MS ISO/IEC 17799:2005

INFORMATION TECHNOLOGY - SECURITY TECHNIQUES - CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT
(FIRST REVISION)
(ISO/IEC 17799:2005, IDT)

ICS: 35.040

Descriptors: general, non-repudiation

© Copyright 2005

DEPARTMENT OF STANDARDS MALAYSIA

MS ISO/IEC 17799:2005

Securing Our Cyberspace

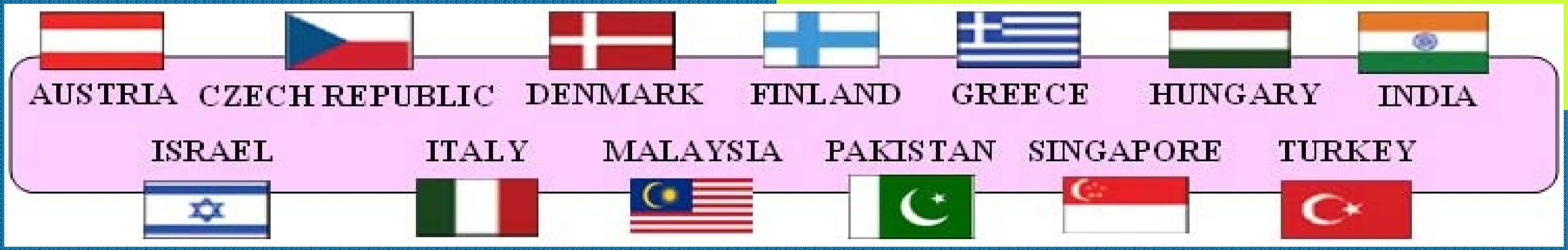
The NATIONAL CYBER SECURITY POLICY
- Cyber Security Technology Framework

Malaysian Common Criteria Evaluation & Certification (MyCC) Scheme

Malaysia was accepted as CCRA Certificate Consuming Participant on 28 March 2007

MISSION

"to <u>increase</u> Malaysia's competitiveness in <u>quality assurance of information security</u> based on the Common Criteria (CC) standard and to build consumers' <u>confidence towards Malaysian information security products</u>"

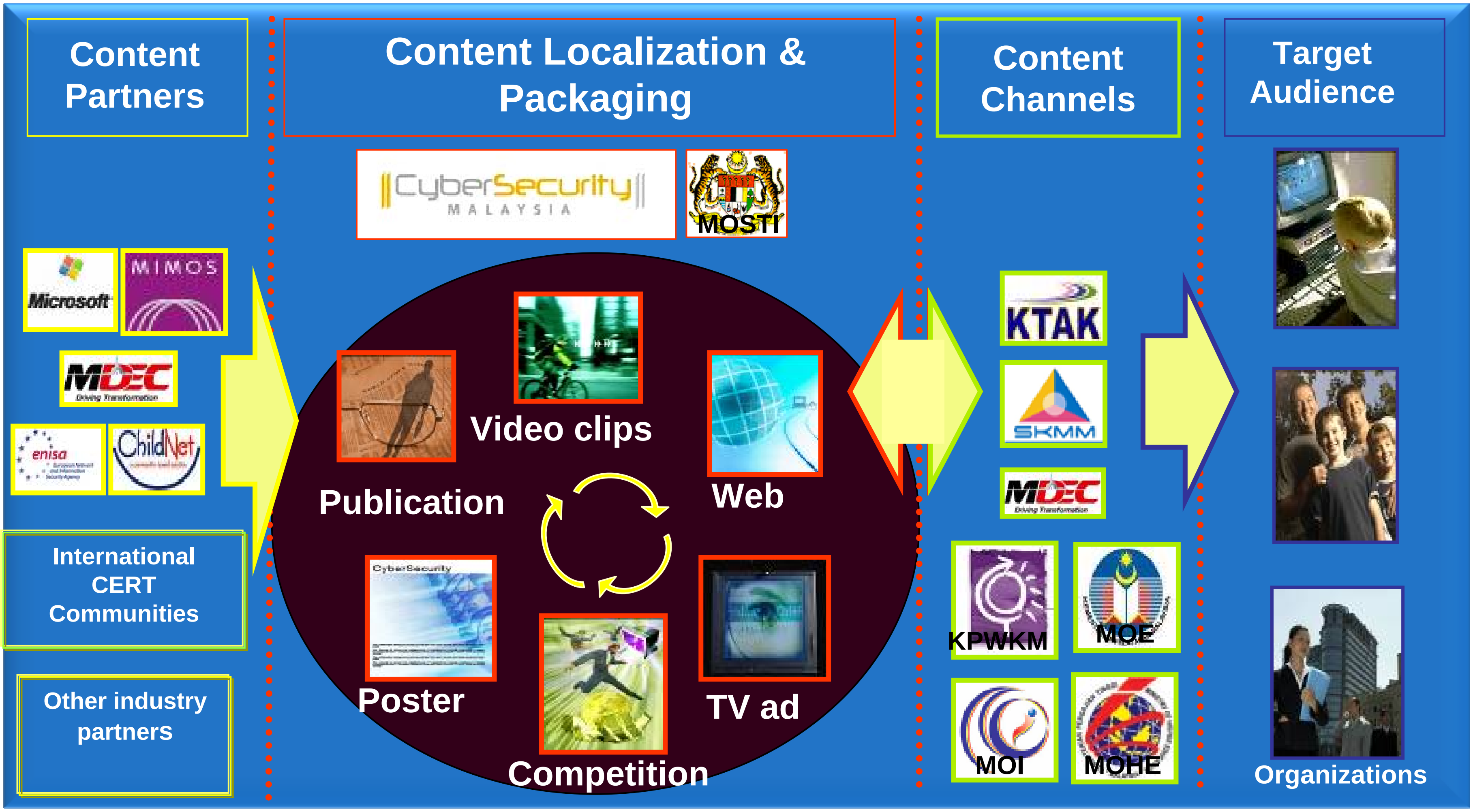


AUSTRIA CZECH REPUBLIC DENMARK FINLAND GREECE HUNGARY INDIA

ISRAEL ITALY MALAYSIA PAKISTAN SINGAPORE TURKEY

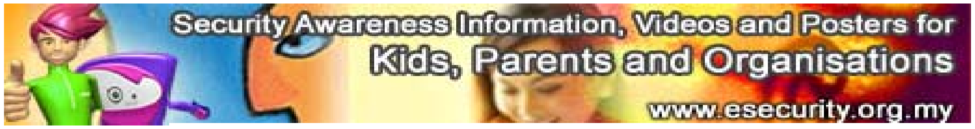
Securing Our Cyberspace

The NATIONAL CYBER SECURITY POLICY
- Culture of Cyber Security & Capacity Building



Securing Our Cyberspace

Let's Make
The Internet
A Safer Place


Security Awareness Information, Videos and Posters for
Kids, Parents and Organisations
www.esecurity.org.my

The NATIONAL CYBER SECURITY POLICY
- Culture of Cyber Security & Capacity Building

CyberSecurity MALAYSIA

Security Professional & Capacity Building

- International Information Systems Security Certification Consortium (ISC2) to promote Certified Information System Security Professional (CISSP) and System Security Certified Professional (SSCP)
- Information Security Audit and Control Association (ISACA) to promote Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM)
- Professional in Critical Infrastructure Protection (PCIP) of the Critical Infrastructure Institute (CII)

CISSP® CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL

SSCP® SYSTEMS SECURITY CERTIFIED PRACTITIONER

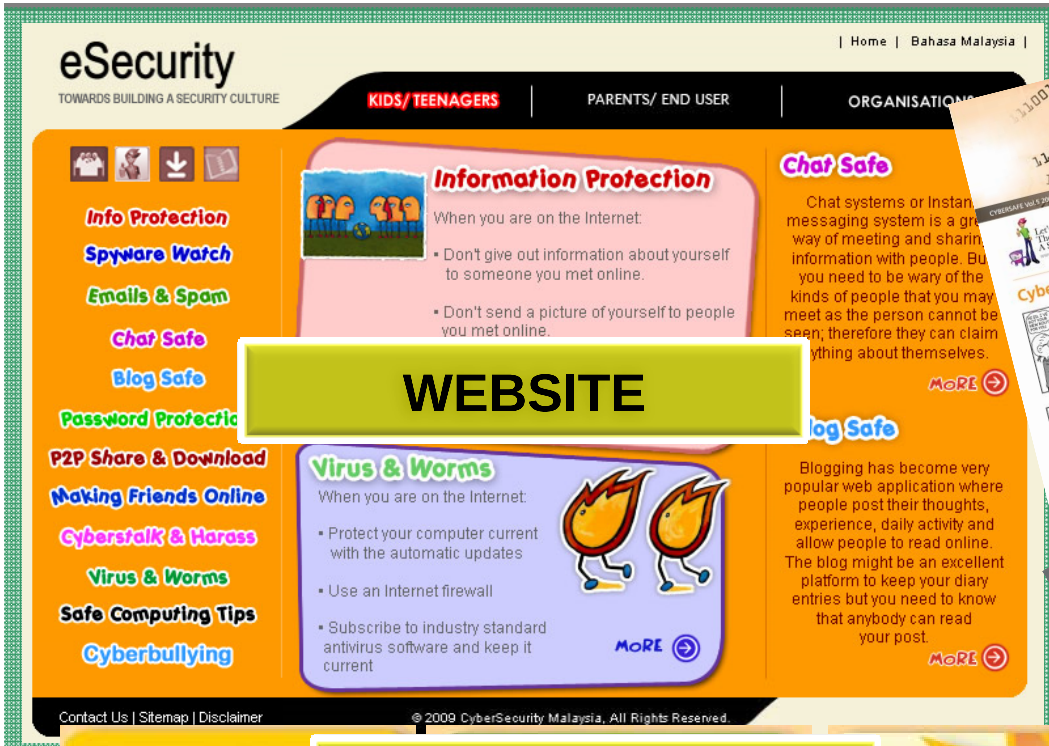
Outreach

Awareness posters
e-security website: www.esecurity.org.my
eSecurity newsletter (published every quarter)
CyberSAFE awareness newsletter
INFOSEC Knowledge Sharing
Radio Advertisements

Securing Our Cyberspace

The NATIONAL CYBER SECURITY POLICY
- Culture of Cyber Security & Capacity Building

CyberSecurity MALAYSIA



| Home | Bahasa Malaysia |

eSecurity
TOWARDS BUILDING A SECURITY CULTURE

KIDS/ TEENAGERS | PARENTS/ END USER | ORGANISATION

- Info Protection
- Spyware Watch
- Emails & Spam
- Chat Safe
- Blog Safe
- Password Protectio
- P2P Share & Download
- Making Friends Online
- Cyberstalk & Harass
- Virus & Worms
- Safe Computing Tips
- Cyberbullying

Information Protection

When you are on the Internet:

- Don't give out information about yourself to someone you met online.
- Don't send a picture of yourself to people you met online.

Chat Safe

Chat systems or Instan messaging system is a gre way of meeting and sharin information with people. Bu you need to be wary of the kinds of people that you may meet as the person cannot be seen; therefore they can claim ything about themselves.

MORE

Virus & Worms

When you are on the Internet:

- Protect your computer current with the automatic updates
- Use an Internet firewall
- Subscribe to industry standard antivirus software and keep it current

MORE

log Safe

Blogging has become very popular web application where people post their thoughts, experience, daily activity and allow people to read online. The blog might be an excellent platform to keep your diary entries but you need to know that anybody can read your post.

MORE

Contact Us | Sitemap | Disclaimer

© 2009 CyberSecurity Malaysia. All Rights Reserved.

WEBSITE

NEWS LETTERS

ONLINE GAMES

Securing Our Cyberspace

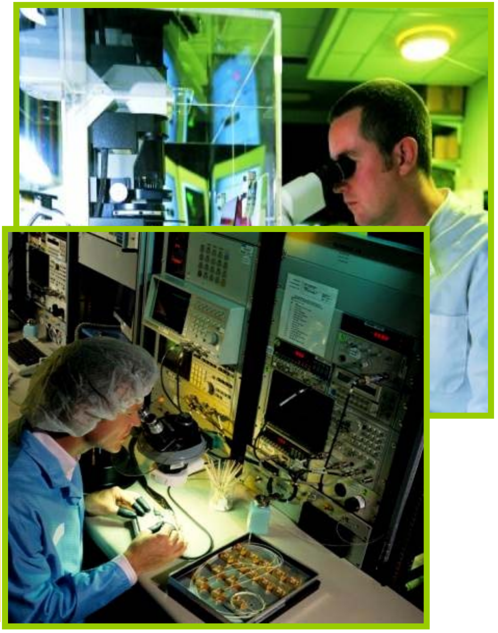
The NATIONAL CYBER SECURITY POLICY
- Research & Development Towards Self Reliance

- To Identify Technologies That Are Relevant and Desirable by the CNII
- Develop Programme to Inculcate Research Culture at the Early Stage Education
- To Collaborate With International R&D Centers, Universities and Partner With
- Local Universities and MIMOS
  Provide Incentives / Bond to the Sponsored Students
- To Established an R&D Institute Specialized in Cyber Security Related Research for CNII

Development of the National R&D Roadmap for Self Reliance in Cyber Security Technologies facilitated by MIMOS

- Handing over ceremony from MIMOS to MOSTI on 27 Nov 2007

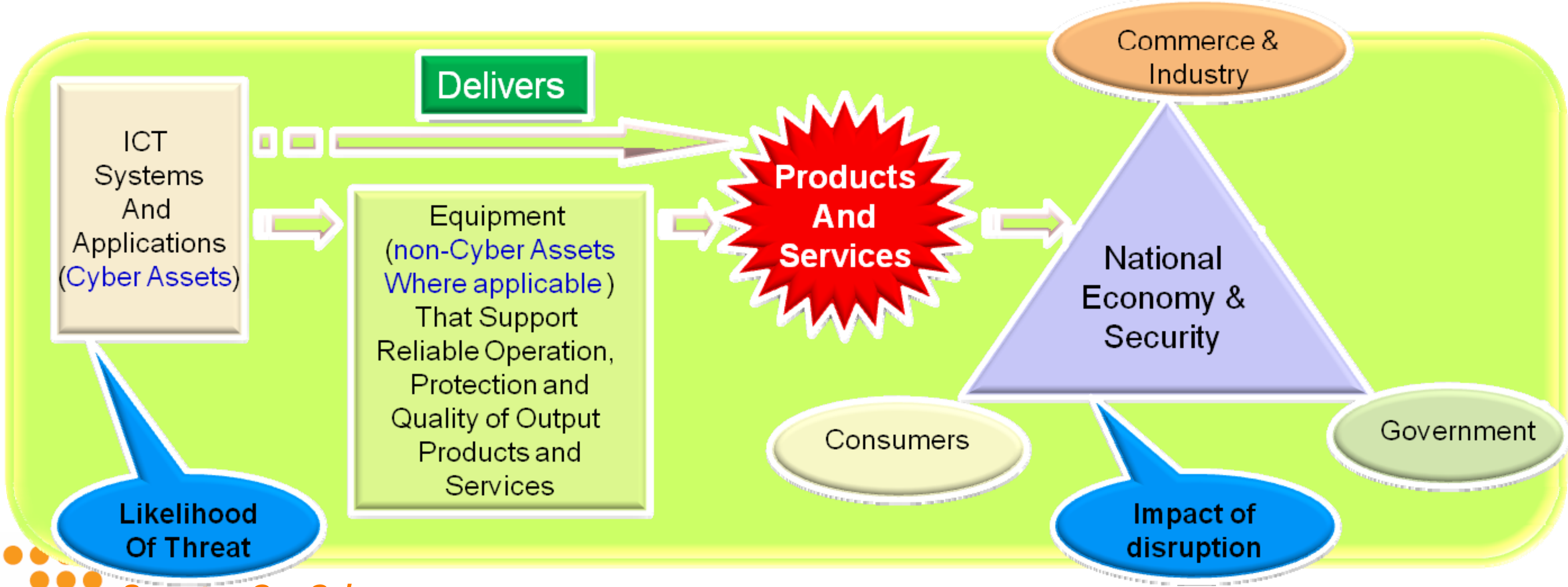
MIMOS



The NATIONAL CYBER SECURITY POLICY
- Compliance & Enforcement

Risk Assessment Focus in NCSP :

Risk Assessment (in NCSP-PT6 context) looks at the **likelihood** of threats exploiting vulnerabilities to **Cyber Assets** disrupting/compromising delivery of **Products and Services** and the **consequence or impact** of the disruption/compromises of the **Products and Services to the Nation**, Commerce, Industry, Government, Consumers and other beneficiaries

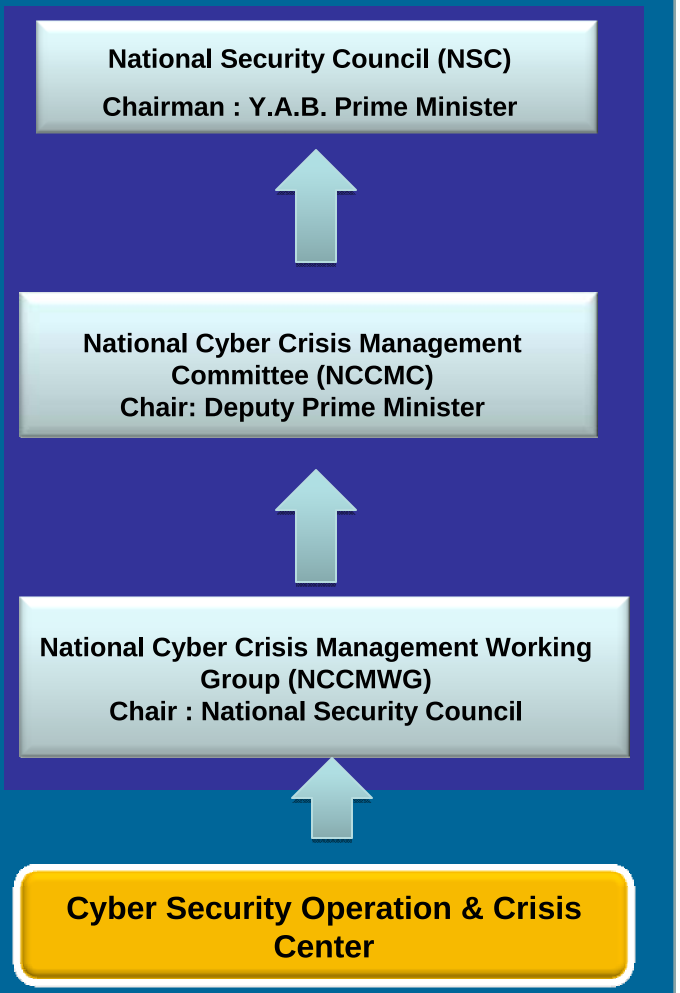

ICT Systems And Applications (Cyber Assets)
Delivers
Equipment (non-Cyber Assets Where applicable) That Support Reliable Operation, Protection and Quality of Output Products and Services
Products And Services
Commerce & Industry
National Economy & Security
Consumers
Government
Likelihood Of Threat
Impact of disruption

Securing Our Cyberspace

THE NATIONAL CYBER SECURITY POLICY
- Cyber Security Emergency Readiness

NATIONAL CYBER CRISIS MANAGEMENT PLAN

Develop the National Cyber Crisis Management **framework** that outlines the **strategy** for cyber attacks mitigation and response among Malaysia's Critical National Information Infrastructure (CNII) through **public and private collaboration and coordination**



National Security Council (NSC)
Chairman : Y.A.B. Prime Minister

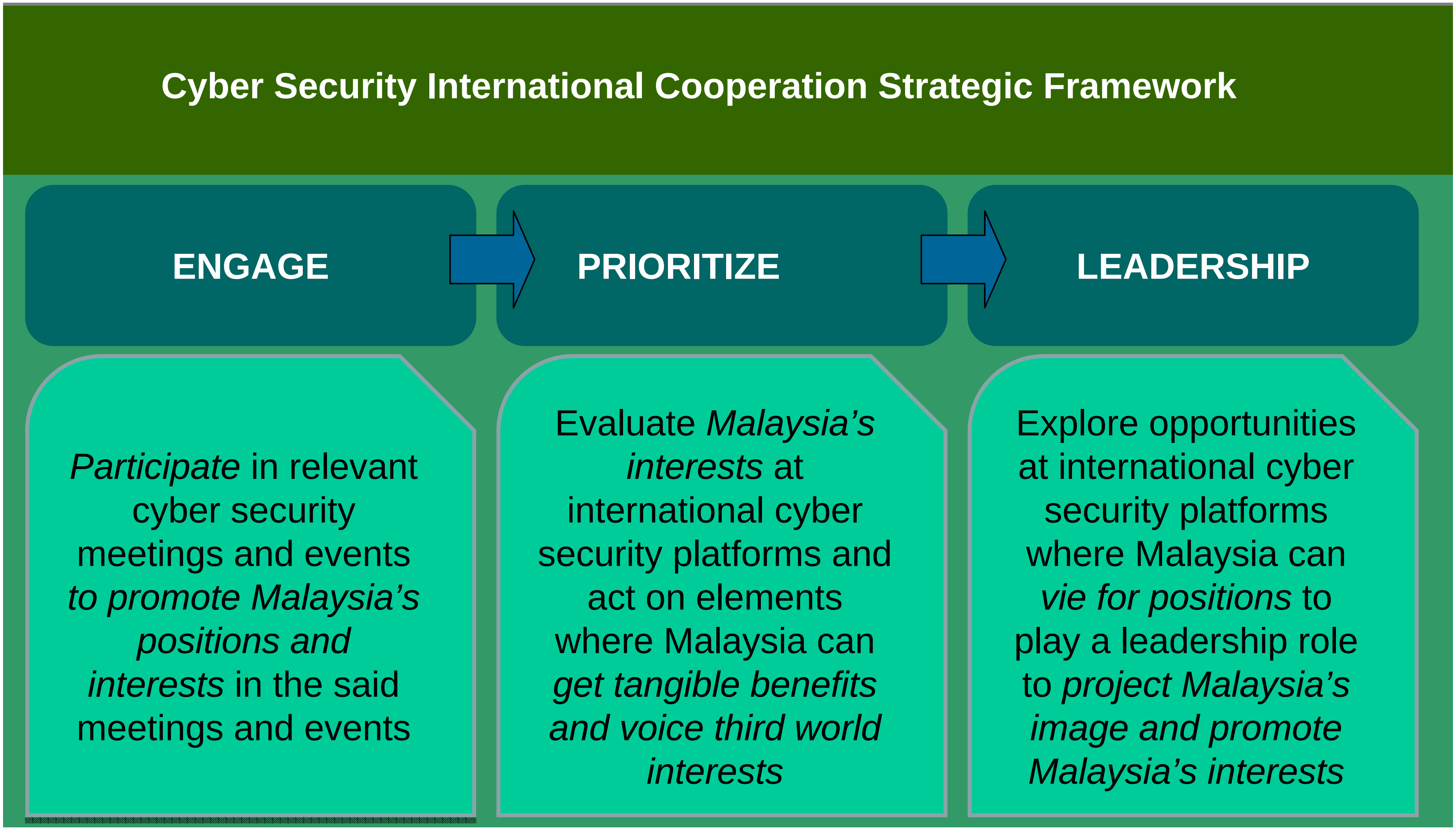
National Cyber Crisis Management Committee (NCCMC)
Chair: Deputy Prime Minister

National Cyber Crisis Management Working Group (NCCMWG)
Chair : National Security Council

Cyber Security Operation & Crisis Center

Securing Our Cyberspace

The NATIONAL CYBER SECURITY POLICY
- International Cooperation



Cyber Security International Cooperation Strategic Framework

ENGAGE

Participate in relevant cyber security meetings and events *to promote Malaysia's positions and interests* in the said meetings and events

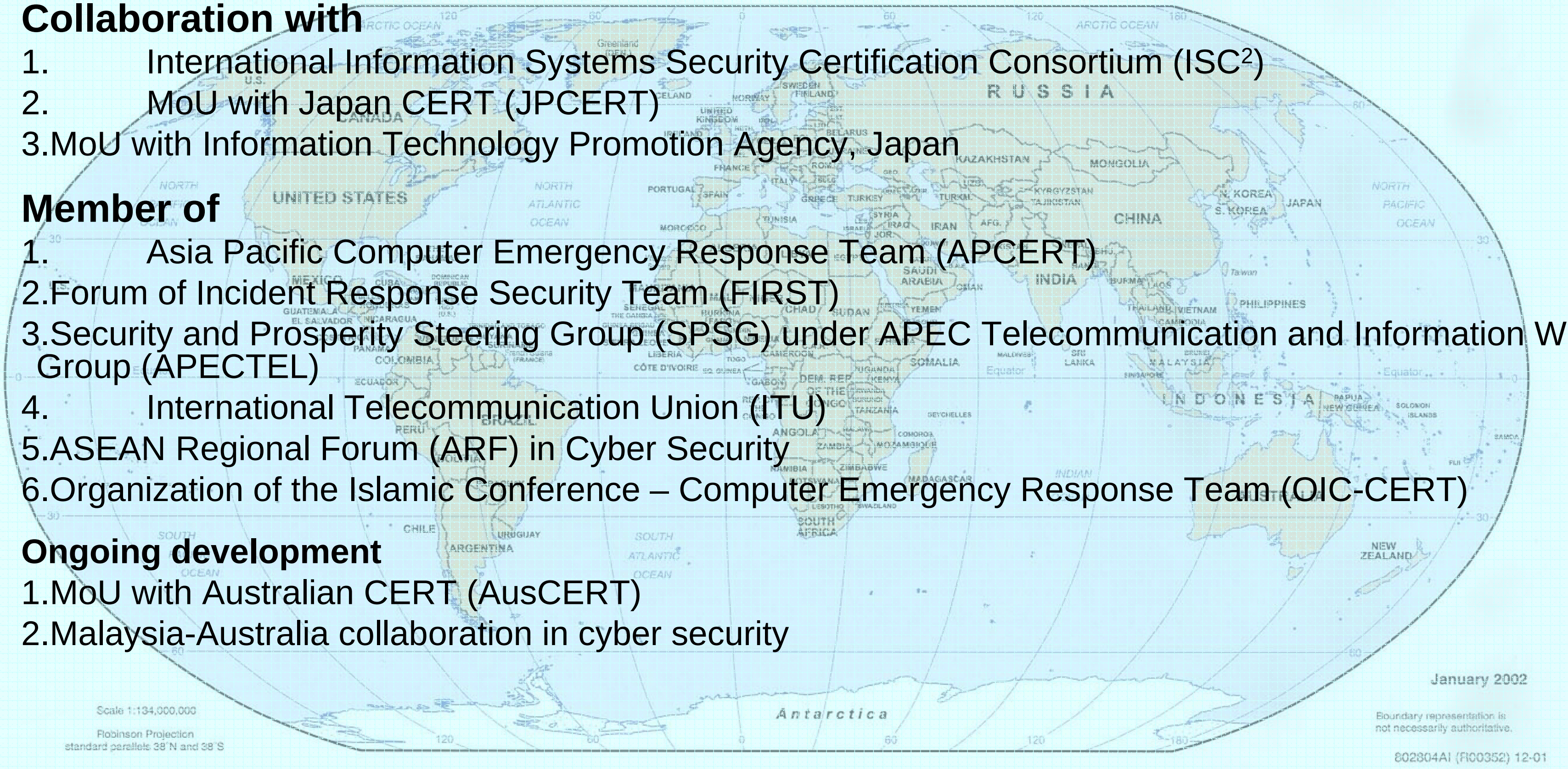
PRIORITIZE

Evaluate *Malaysia's interests* at international cyber security platforms and act on elements where Malaysia can *get tangible benefits and voice third world interests*

LEADERSHIP

Explore opportunities at international cyber security platforms where Malaysia can *vie for positions* to play a leadership role to *project Malaysia's image and promote Malaysia's interests*

The NATIONAL CYBER SECURITY POLICY
- International Cooperation



Collaboration with

1. International Information Systems Security Certification Consortium (ISC^2)
2. MoU with Japan CERT (JPCERT)
3. MoU with Information Technology Promotion Agency, Japan

Member of

1. Asia Pacific Computer Emergency Response Team (APCERT)
2. Forum of Incident Response Security Team (FIRST)
3. Security and Prosperity Steering Group (SPSG) under APEC Telecommunication and Information Working Group (APECTEL)
4. International Telecommunication Union (ITU)
5. ASEAN Regional Forum (ARF) in Cyber Security
6. Organization of the Islamic Conference – Computer Emergency Response Team (OIC-CERT)

Ongoing development

1. MoU with Australian CERT (AusCERT)
2. Malaysia-Australia collaboration in cyber security

The NATIONAL CYBER SECURITY POLICY
- International Cooperation

ESTABLISHMENT OF OIC-CERT ORGANISATION

1) Collaboration of Computer Emergency Response Team (CERT) among OIC member countries.

2)Resolution of 35th Session Council of Foreign Minister of the OIC, Kampala, Uganda 18-20 May 2008

3)Established in January 2009 with 15 member countries
Chair : Malaysia – CyberSecurity Malaysia
Secretariat : Tunisia – Tunisia National Agency for Computer Security

Members : 1) Saudi Arabia 2) Pakistan
3) Nigeria 4) Iran
5) Egypt 6) Morocco
7) Libya 8) Brunei
9) Indonesia 10) Jordan
11) Oman 12) Syria
13) Bangladesh 14)Turkey

OIC-CERT
Computer Emergency Response Team

KL Resolution 2009

- ❑ the OIC-CERT Term of Reference tabled during this AGM is accepted
- ❑ the appointments of the OIC-CERT Steering Committee for the term of 2009-2011
- ❑ the OIC-CERT will intensify efforts in areas of:
  i. Strategic Cooperation
  ii. Technical Cooperation
  iii. Awareness & Capacity Building
  iv. Law Enforcement & Regulatory Cooperation
  v. Funding

The NATIONAL CYBER SECURITY POLICY
- International Cooperation

OIC-CERT
Computer Emergency Response Team

13 – 15 Jan 2009

OIC-CERT 1ST Information Security Seminar 2009 with a theme STRATEGIC PARTNERSHIP AGAINST CYBER THREATS targeting ICT security professionals, policy makers, industry players and from the OIC member researchers countries.

❑ 14 – 15 Jan 2009, OIC-CERT 1st Annual General meeting. Agenda:

- Approval of the OIC-CERT Term of Reference
- Appointment of Steering Committee Members
- Discussion on OIC-CERT Strategic Direction
- Discussion on OIC-CERT Website
- Accepta

Strategic Partnership Against Cyber Threats
OIC-CERT SEMINAR 2009
Officiated by
Y.B. Datuk Dr. Maximus Johnity Ongkili
13 - 15 January 2009
Plaza Mutiara, Kuala Lumpur

Securing Our Cyberspace

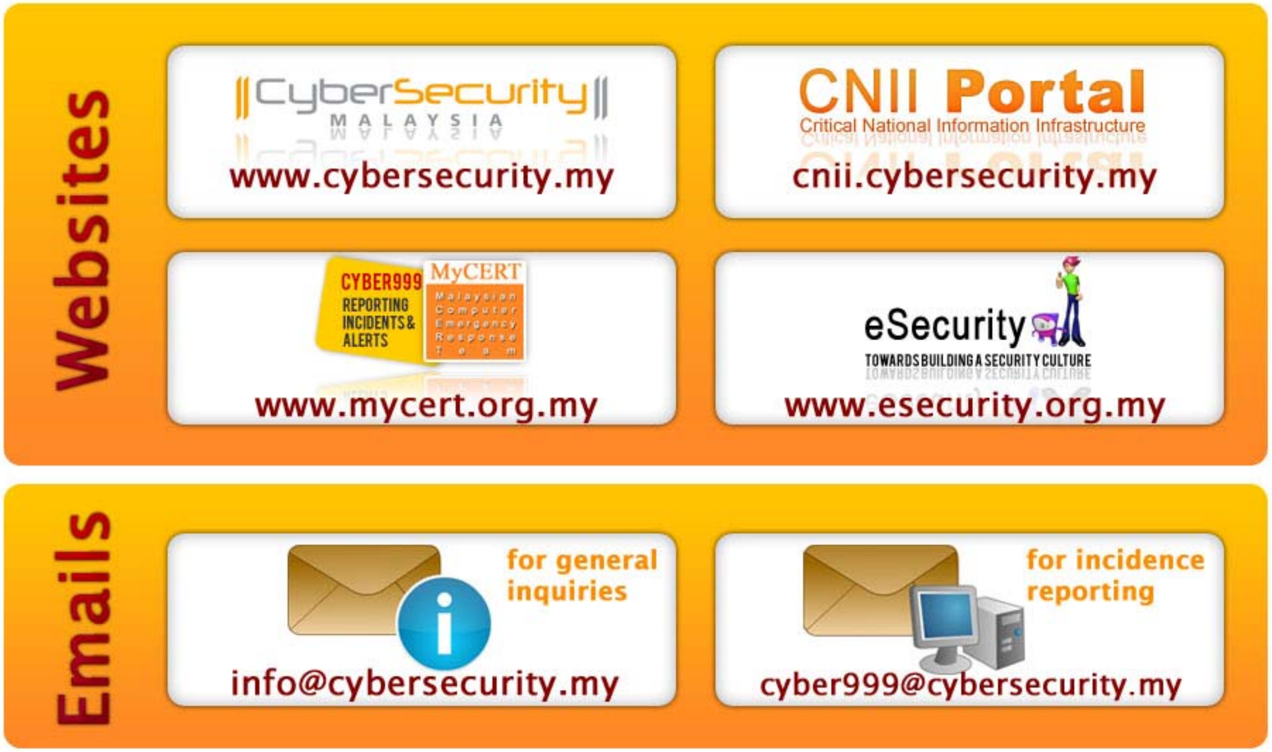
The NATIONAL CYBER SECURITY POLICY
- International Cooperation

OBJECTIVE OF OIC-CERT

- Strengthen relationship amongst CERT/CSIRT in the OIC countries
- Information sharing
- Prevent/reduce cyber terrorism activities
- Education and Outreach ICT Security Programs
- Promote collaborative technology research, development and innovations
- Promote Good Practices and / or recommendation to address legal and regulatory issues
- Assist member countries to establish National CERTs

ACCEPTED AS OIC AFFILIATED ORGANIZATION IN THE 36th Session Council of Foreign Minister of the OIC, Damsyik, Syria 21-23 May 2009

Securing Our Cyberspace


CyberSecurity MALAYSIA
CNII Portal
Critical National Information Infrastructure
CYBER999
REPORTING INCIDENTS & ALERTS
MyCERT
Malaysian Computer Emergency Response Team
eSecurity
TOWARDS BUILDING A SECURITY CULTURE

Websites

www.cybersecurity.my

cnii.cybersecurity.my

www.mycert.org.my

www.esecurity.org.my

Emails

for general inquiries
info@cybersecurity.my

for incidence reporting
cyber999@cybersecurity.my