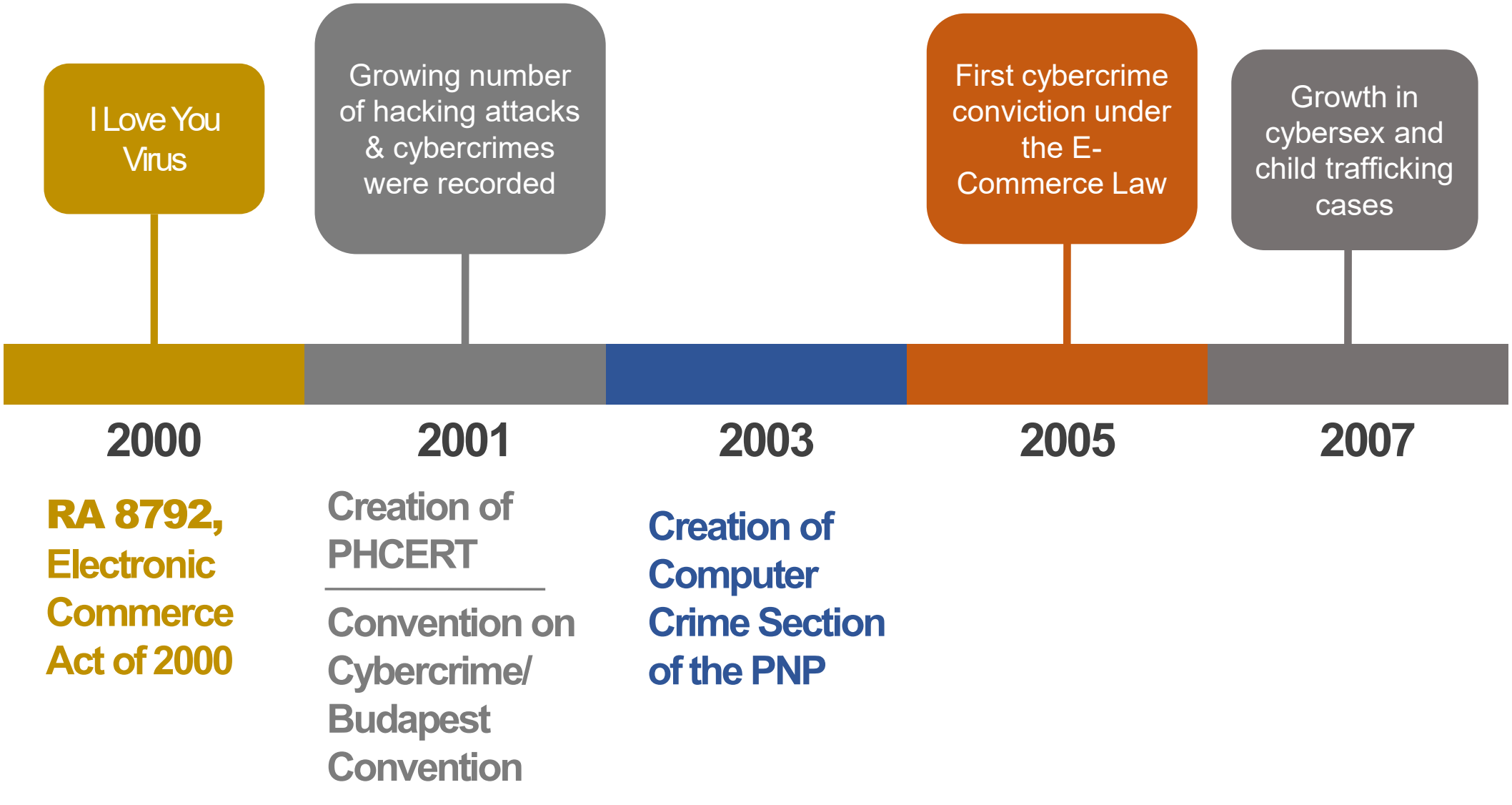
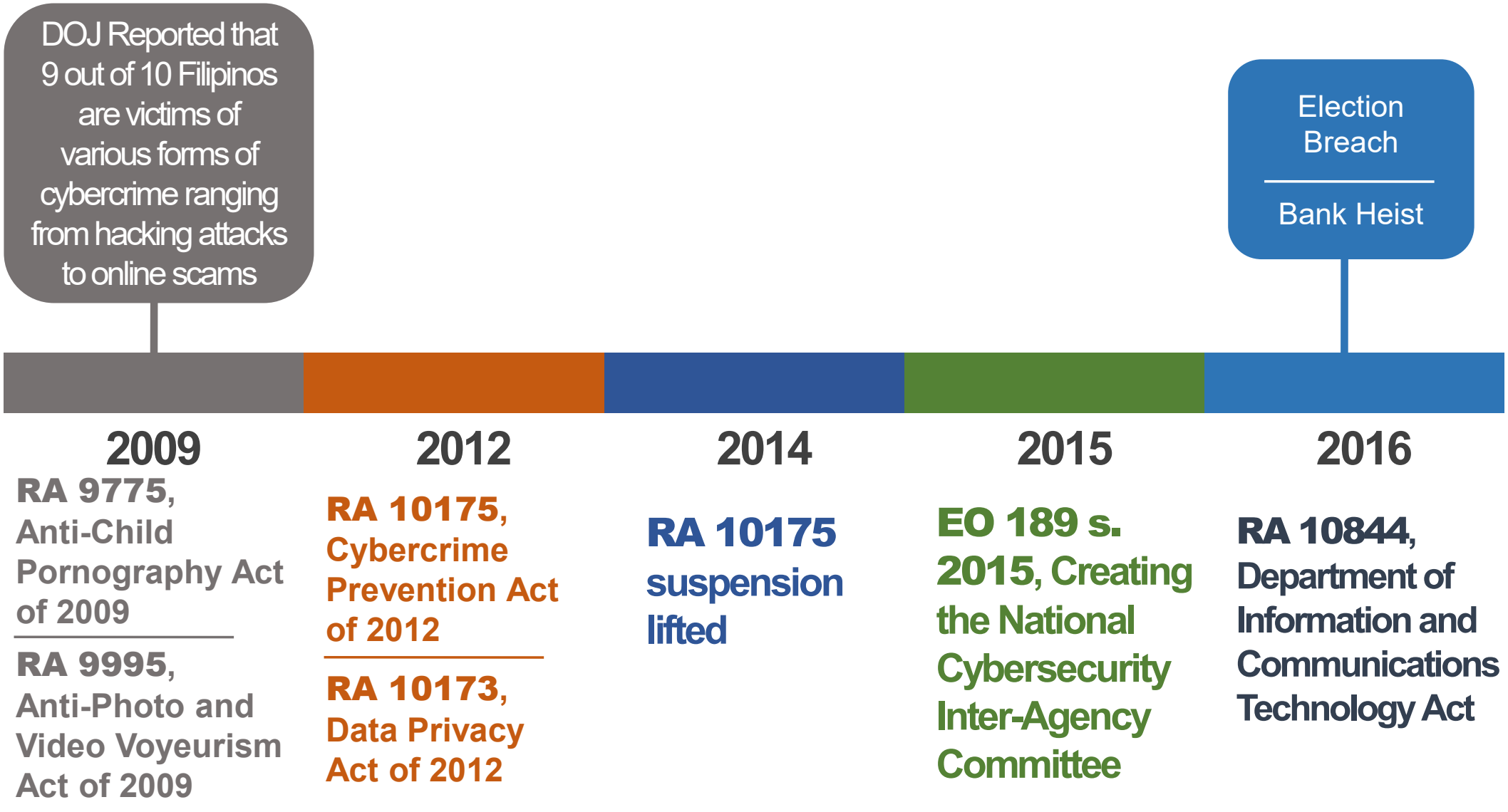
THE PHILIPPINES'

CYBERSECURITY LAWS, BEST PRACTICES, AND STRATEGIES

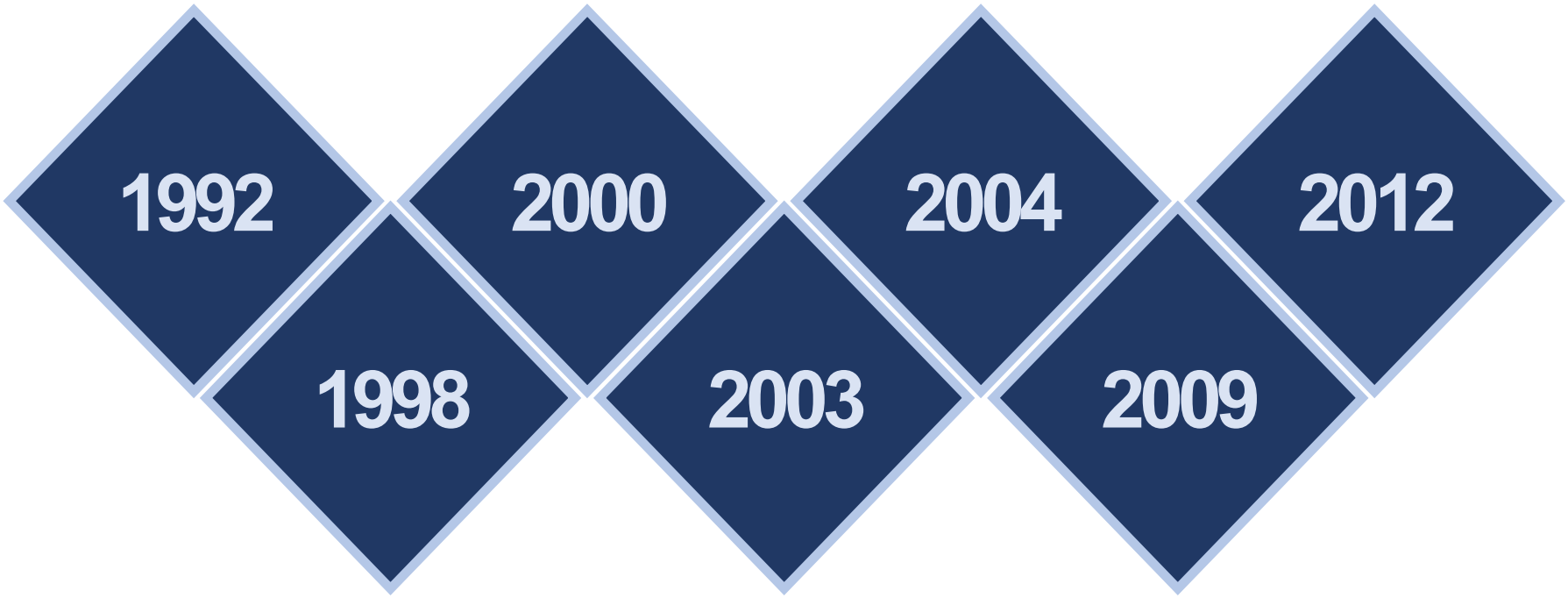
DR. THELMA D. VILLAMOREL, PECE
OIC – Division Chief
Critical Infostructure Evaluation and
Cybersecurity Standards Monitoring Division
Cybersecurity Bureau
thelma.villamorel@dict.gov.ph



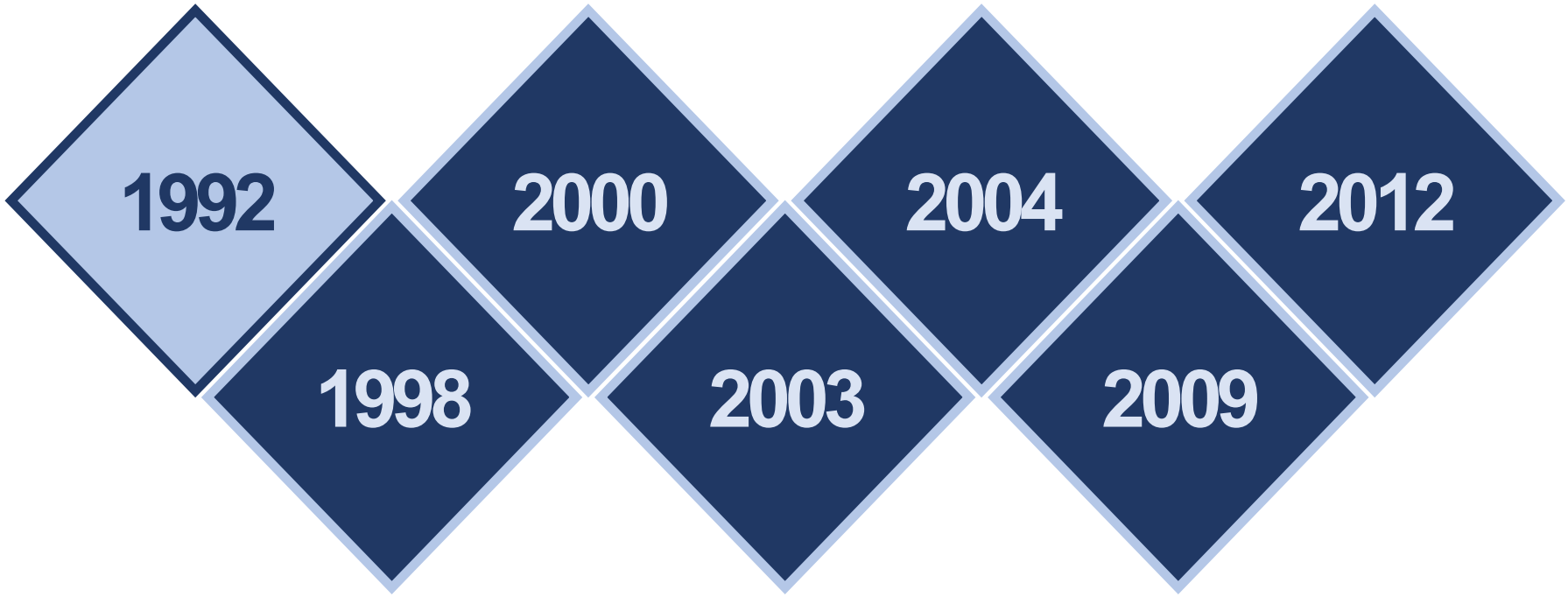
HISTORY OF CYBERSECURITY IN THE PHILIPPINES



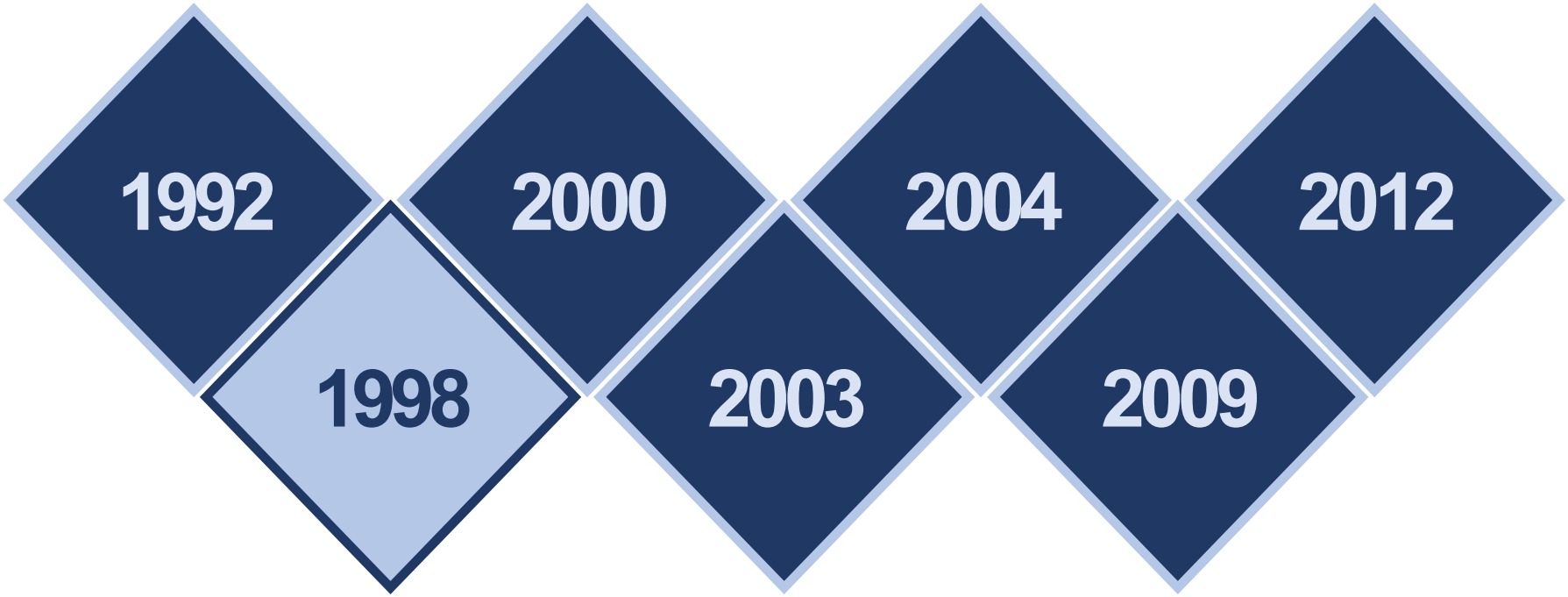
HISTORY OF CYBERSECURITY IN THE PHILIPPINES



Laws enacted that are technology-related

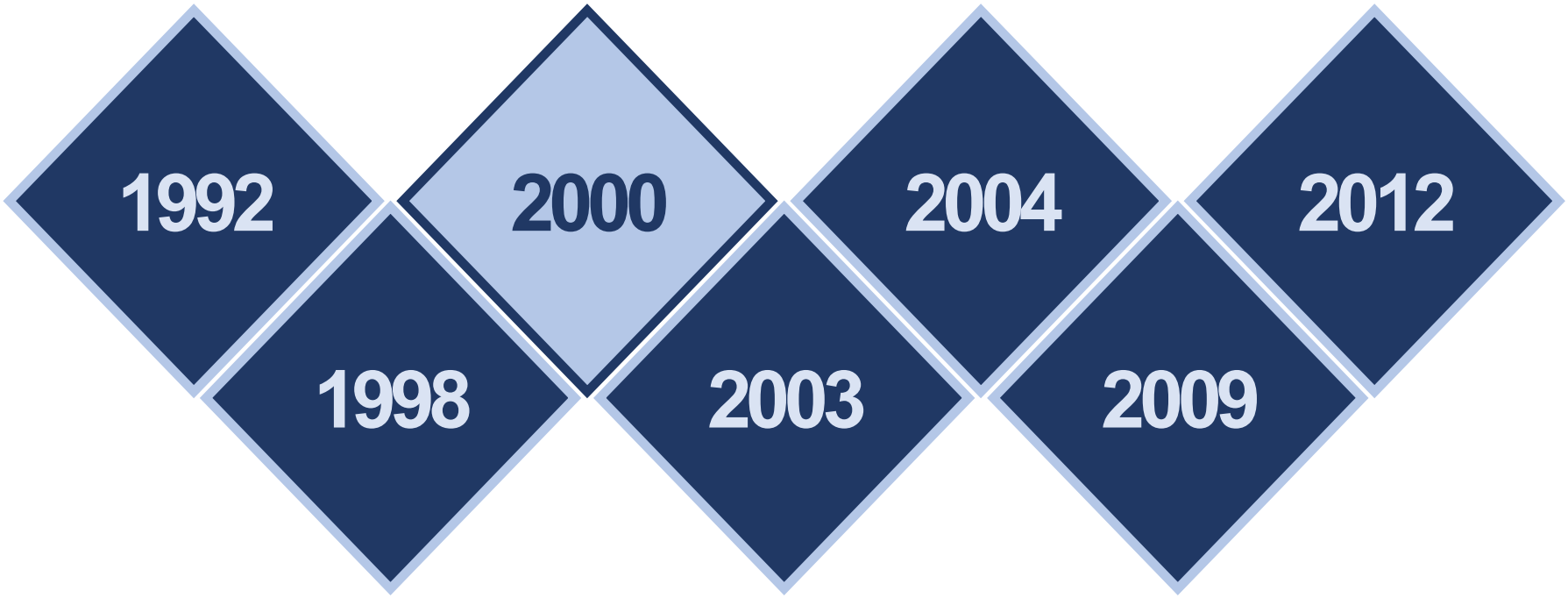


RA 7610
Special Protection of Children against Abuse Act



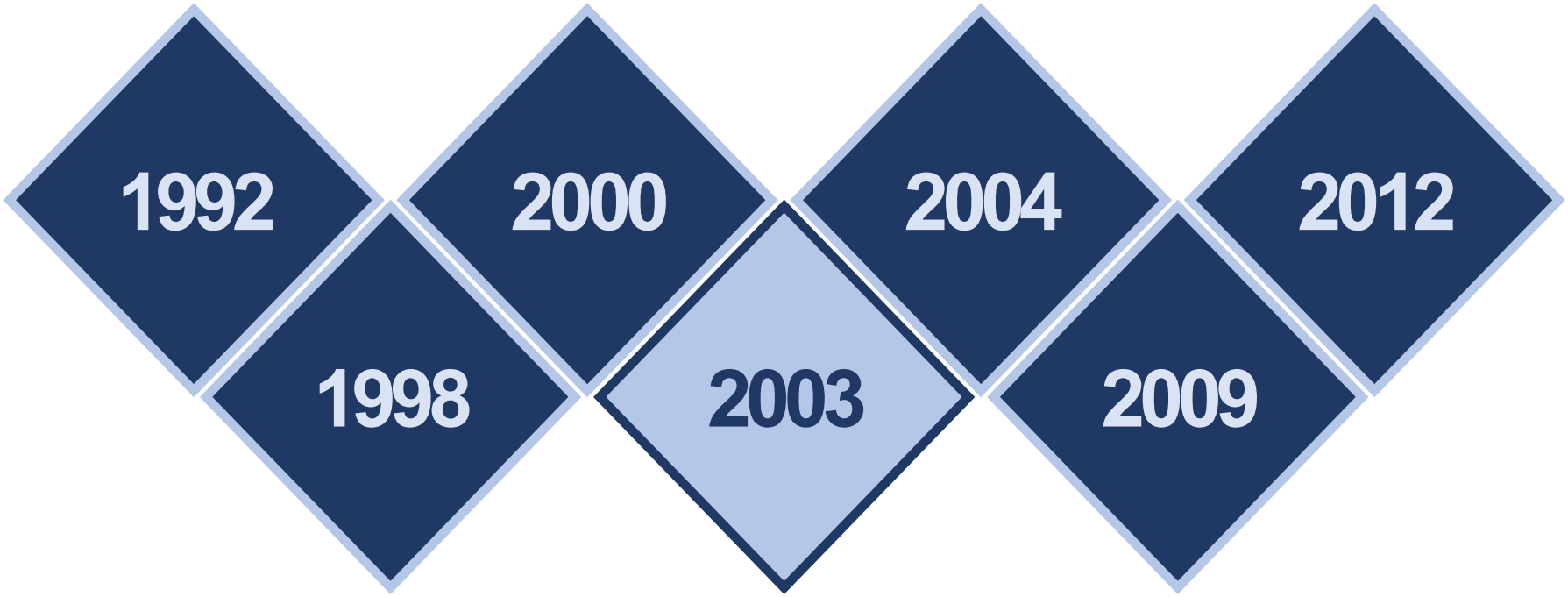
RA 8484

Access Devices Regulation Act



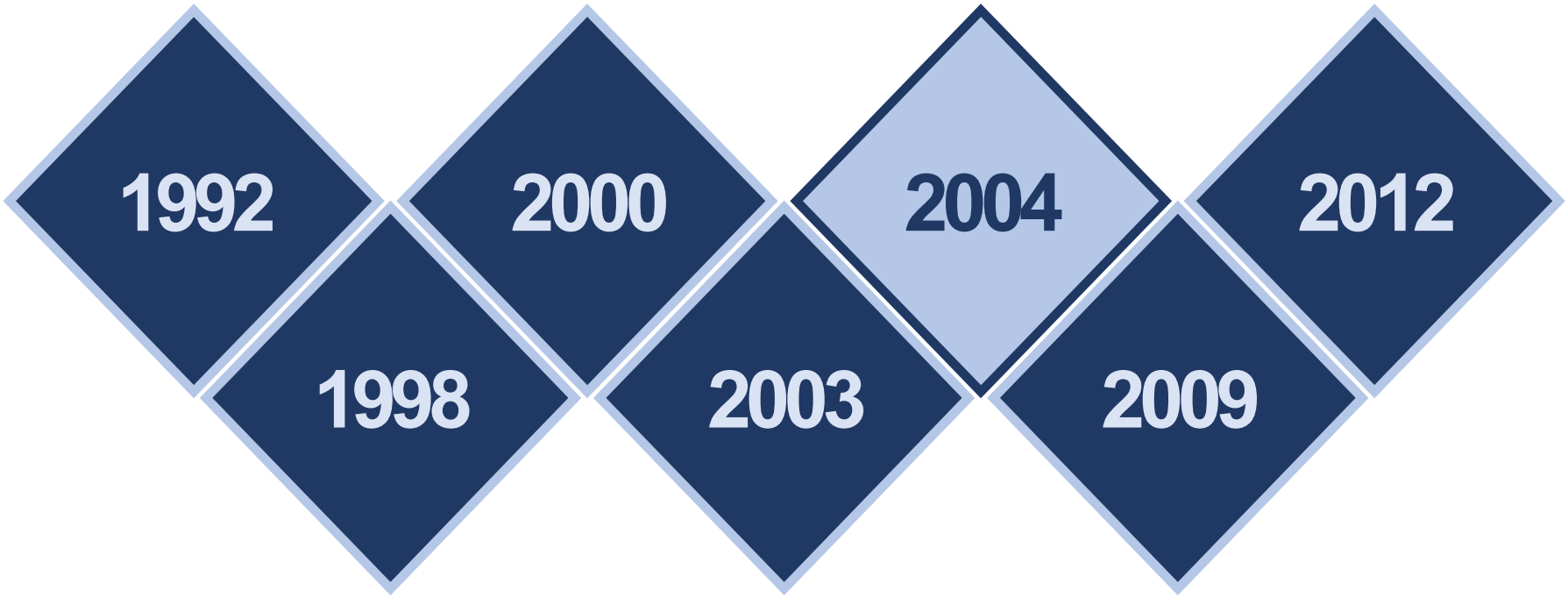
RA 8792

Electronic Commerce Act



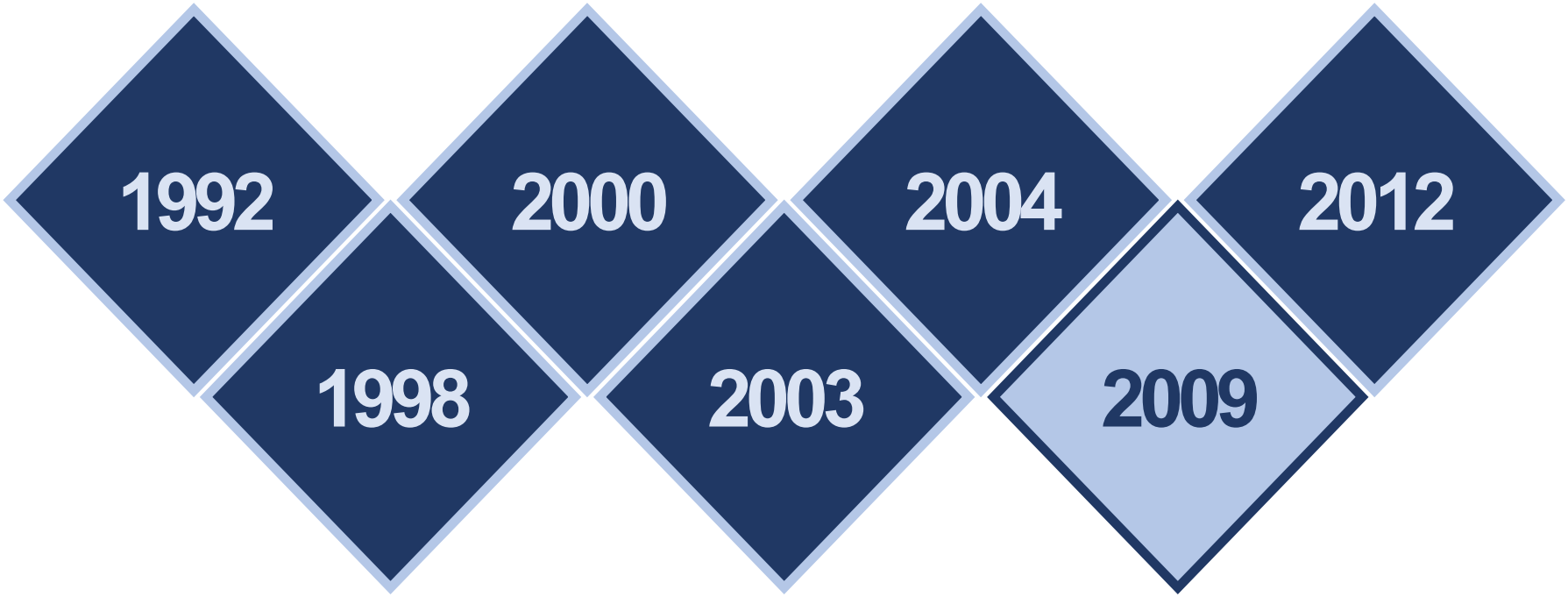
RA 9208

Anti-Trafficking Act



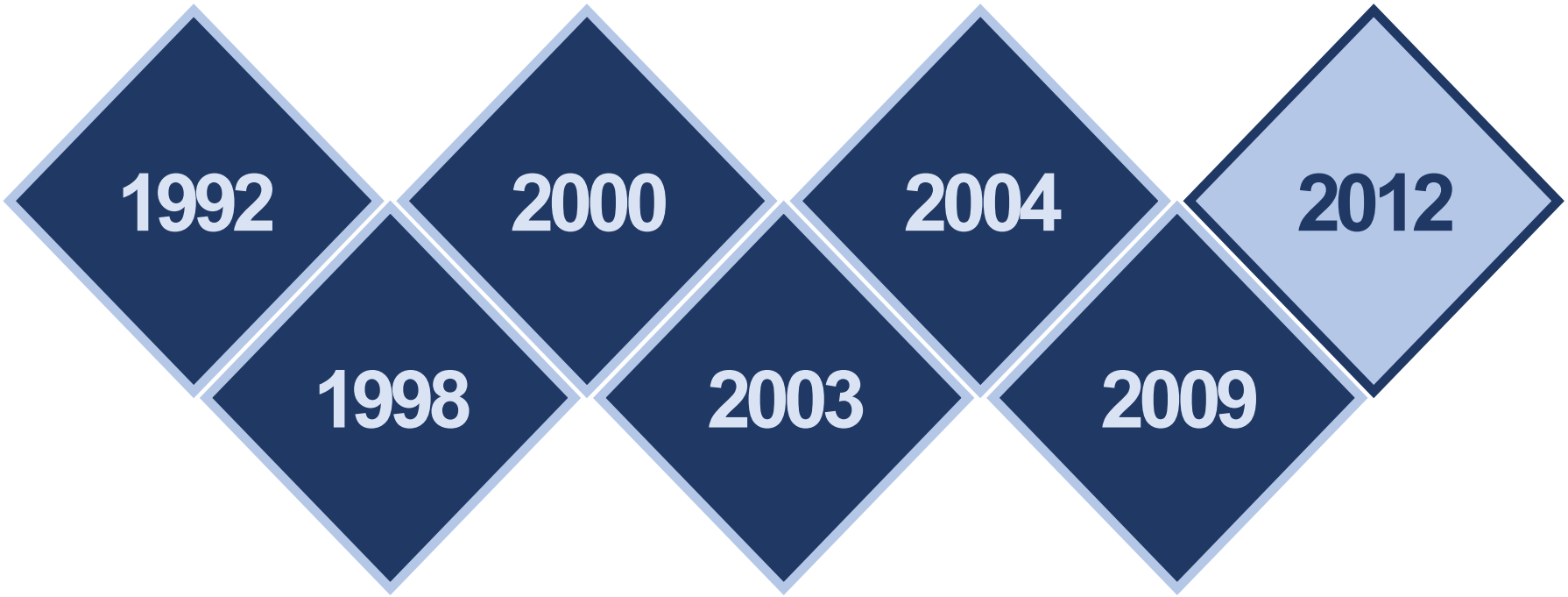
RA 9262

Anti-Violence against Women and Children Act



RA 9775
Anti-Child Pornography Act

RA 9995
Anti-Photo and Video Voyeurism



RA 10173
Data Privacy Act

RA 10175
Cybercrime Prevention Act

CyberSecurity in the Philippines should be divided according to its major **CyberSecurity Responsibilities:** Law Enforcement, Protection and National Defense

Community	Agency/ Organization	Emphasis
Law Enforcement	**DOJ-NBI DILG-PNP**	Identify Criminals Preserve Evidence Prosecute
Network Protection	**DICT CICC**	Disseminate Broadly Ensure Timely Release
National Defense	**DND / AFP NSC**	Defend the Country Protect Military Networks
Intelligence Community	**NICA**	Attribution Advise and Inform Decision Makers

12-PT NATIONAL SECURITY STRATEGY GOALS 2018

Security and Development for Transformational Change and Well-Being of the Filipino People

Guarantee public safety and achieve good governance

Mitigate the impact of health related threats

Develop a dynamic, inclusive, and sustainable economy

Achieve food and water security

Safeguard and preserve national sovereignty and territorial integrity

Heighten consciousness and pride on Filipino heritage, culture and values

Promote human and ecological security

Achieve energy security

Ensure maritime and airspace security

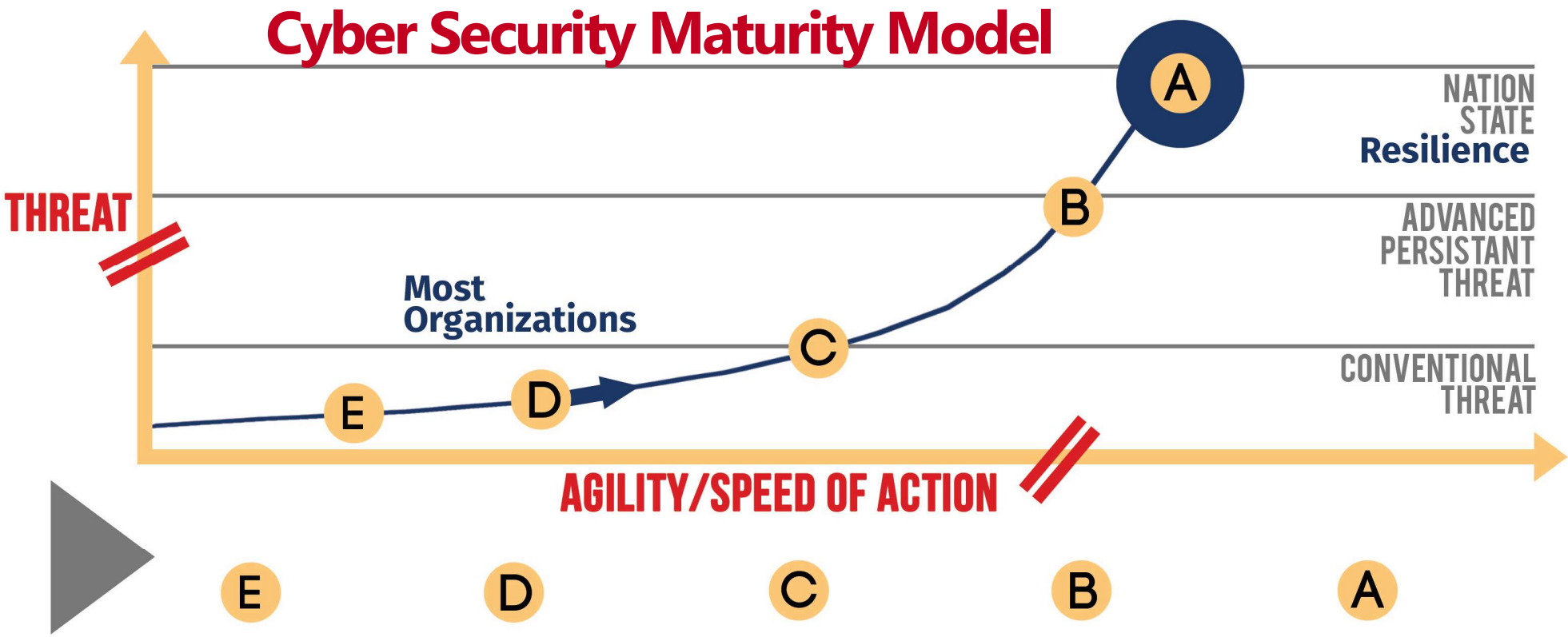
Strengthen international relations

Provide strong cyber infrastructure and cyber security

Improve vital transportation infrastructure and port security

Attacks to CII	**B**ank Heist, **N**avigation Systems Manipulation, **C**ontrol of Electronic Medical Equipment and Records, **O**verride of Oil and Gas Systems
Attacks to Government Infostructure	**H**acking resulting in Data breach **D**efacement of PH Government Agencies Websites
Sophistication of Cyber Attacks	**A**PT, **D**DoS, **S**PAM, **S**pear Phishing, **S**ocial Engineering

Cyber Security Maturity Model



E

REACTIVE & MANUAL

People based following doctrine and doing there best to "put out fires"

D

TOOLS-BASED

Applying tools and technologies piecemeal to assist people in reacting faster

C

INTEGRATED PICTURE

Loosely intergrated with focus on interoperability and standards-based data exchange for IA situational awareness

B

DYNAMIC DEFENSE

Predictive and agile, the enterprise instantiates policy, illuminates events, and helps the operators find, fix, and target for response

A

RESILIENT ENTERPRISE

Predictive and mission focused, isolates and contains damage, secure supply chains, and protext key critical infrastructures to operate through cyber attack

*Source: Presentation of **Robert Lentz** Former CISO US Department of Defense*

Cybersecurity STRATEGY

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

Where are we now?

- Tools based
- Reactive / Manual

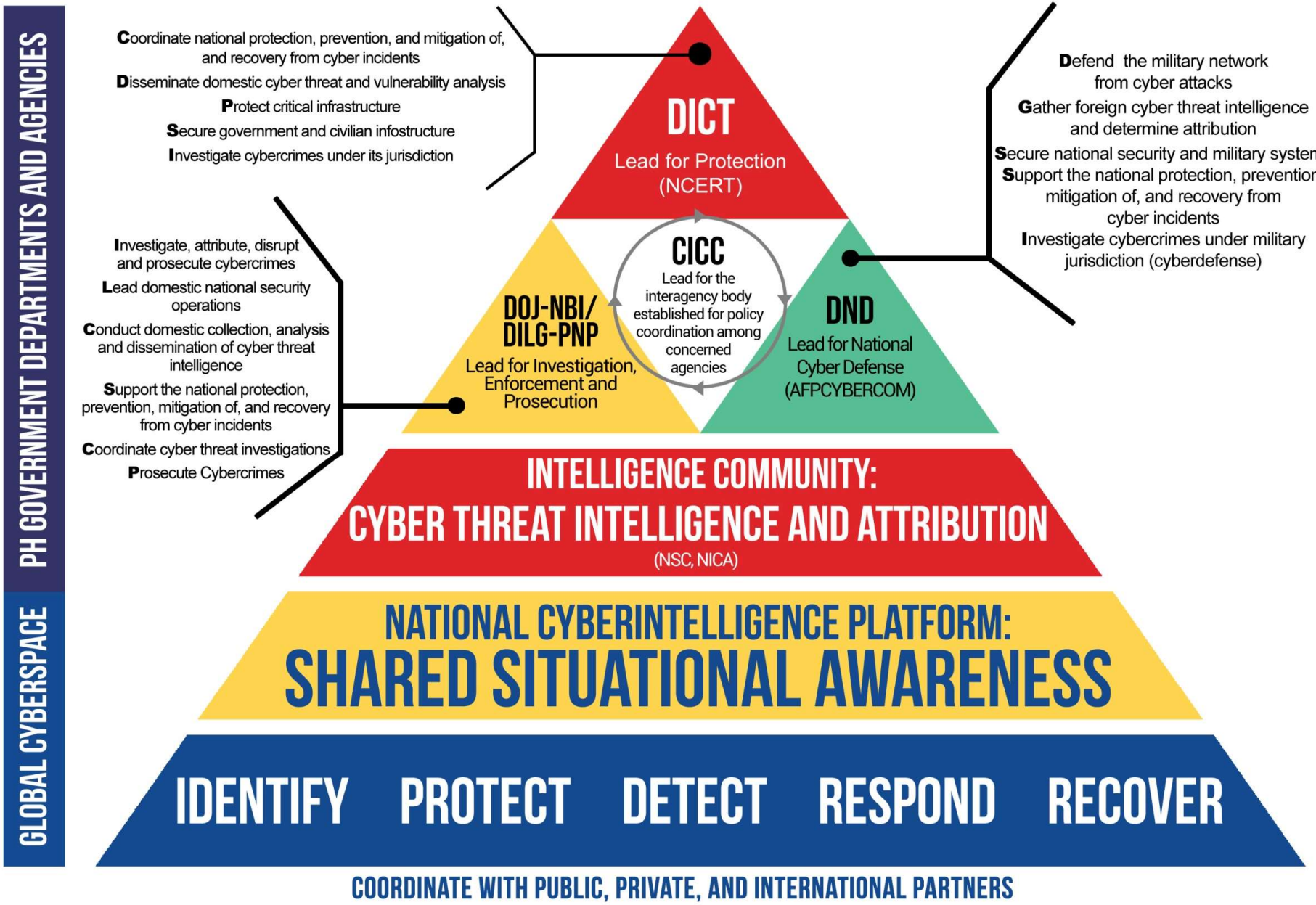
Cyber Resilient Philippines

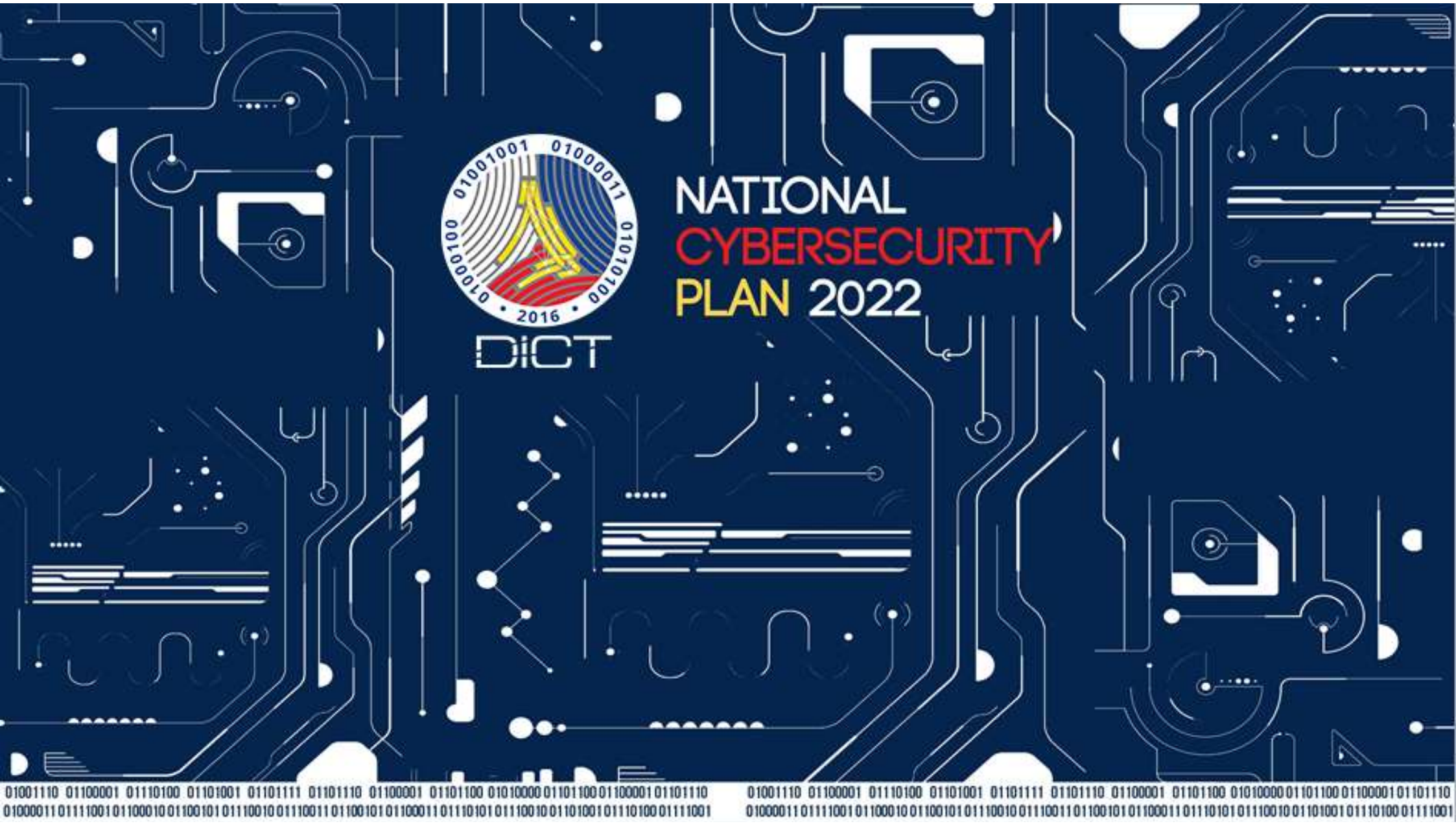
What do we want to achieve?

How do we get there?

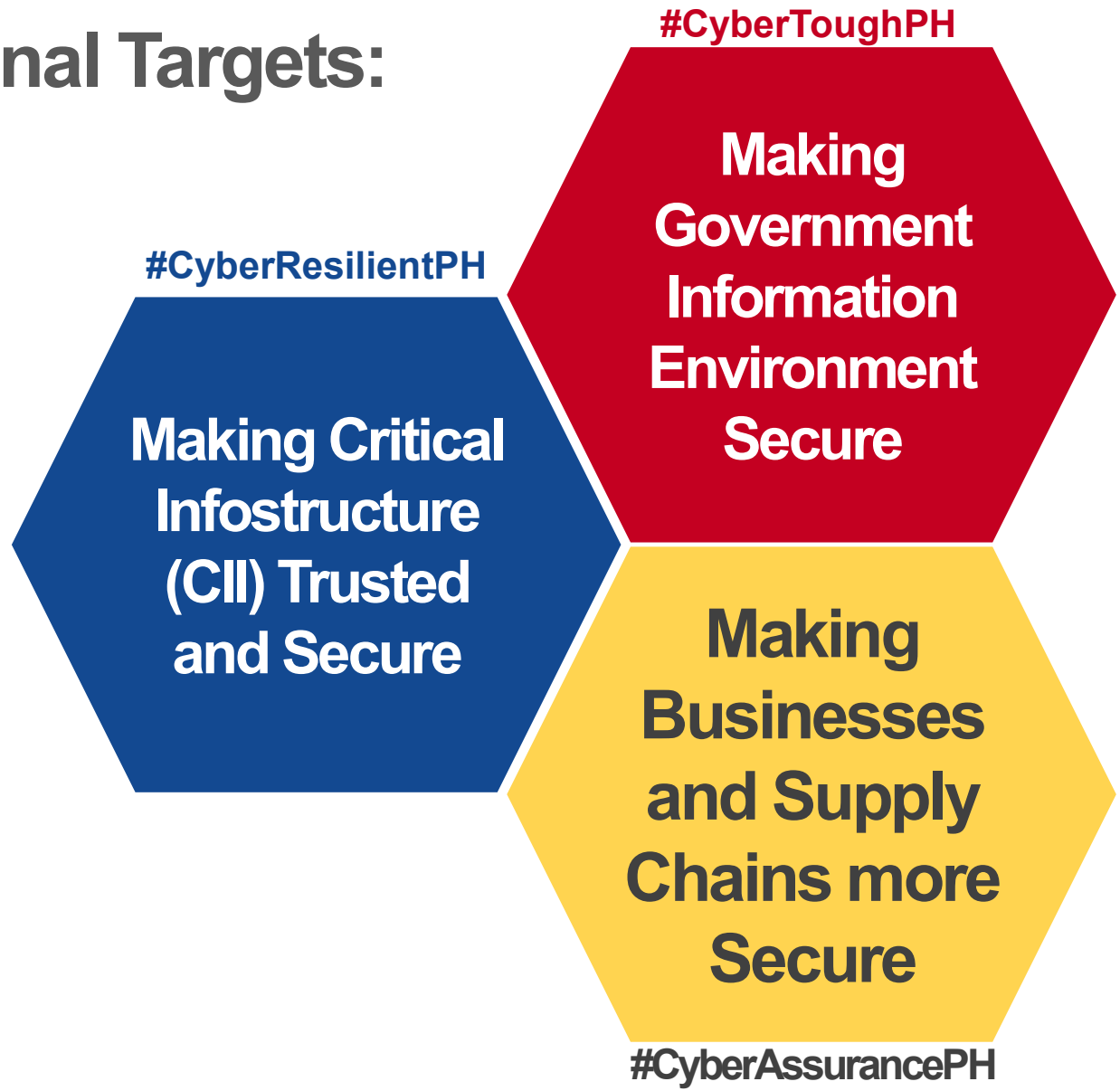
- Crafting of the National CyberSecurity Strategy, Policies, Plans and Programs
- Establishment of NCERT and Implementation of other Programs defined in the National Cybersecurity Plan


The National
CYBER
SECURITY
GOVERNANCE
FRAMEWORK


PH GOVERNMENT DEPARTMENTS AND AGENCIES
GLOBAL CYBERSPACE
Coordinate national protection, prevention, and mitigation of, and recovery from cyber incidents
Disseminate domestic cyber threat and vulnerability analysis
Protect critical infrastructure
Secure government and civilian infostructure
Investigate cybercrimes under its jurisdiction
DICT
Lead for Protection (NCERT)
Defend the military network from cyber attacks
Gather foreign cyber threat intelligence and determine attribution
Secure national security and military systems
Support the national protection, prevention, mitigation of, and recovery from cyber incidents
Investigate cybercrimes under military jurisdiction (cyberdefense)
Investigate, attribute, disrupt and prosecute cybercrimes
Lead domestic national security operations
Conduct domestic collection, analysis and dissemination of cyber threat intelligence
Support the national protection, prevention, mitigation of, and recovery from cyber incidents
Coordinate cyber threat investigations
Prosecute Cybercrimes
CICC
Lead for the interagency body established for policy coordination among concerned agencies
DOJ-NBI/ DILG-PNP
Lead for Investigation, Enforcement and Prosecution
DND
Lead for National Cyber Defense (AFPCYBERCOM)
INTELLIGENCE COMMUNITY:
CYBER THREAT INTELLIGENCE AND ATTRIBUTION
(NSC, NICA)
NATIONAL CYBERINTELLIGENCE PLATFORM:
SHARED SITUATIONAL AWARENESS
IDENTIFY PROTECT DETECT RESPOND RECOVER
COORDINATE WITH PUBLIC, PRIVATE, AND INTERNATIONAL PARTNERS


01001001 01000011
01010100 01000100
2016
DICT
NATIONAL
CYBERSECURITY
PLAN 2022
01001110 01100001 01110100 01101001 01101111 01101110 01100001 01101100 01010000 01101100 01100001 01101110
01000011 01111001 01100010 01100101 01110010 01110011 01100101 01100011 01110101 01110010 01101001 01110100 01111001

National Targets:

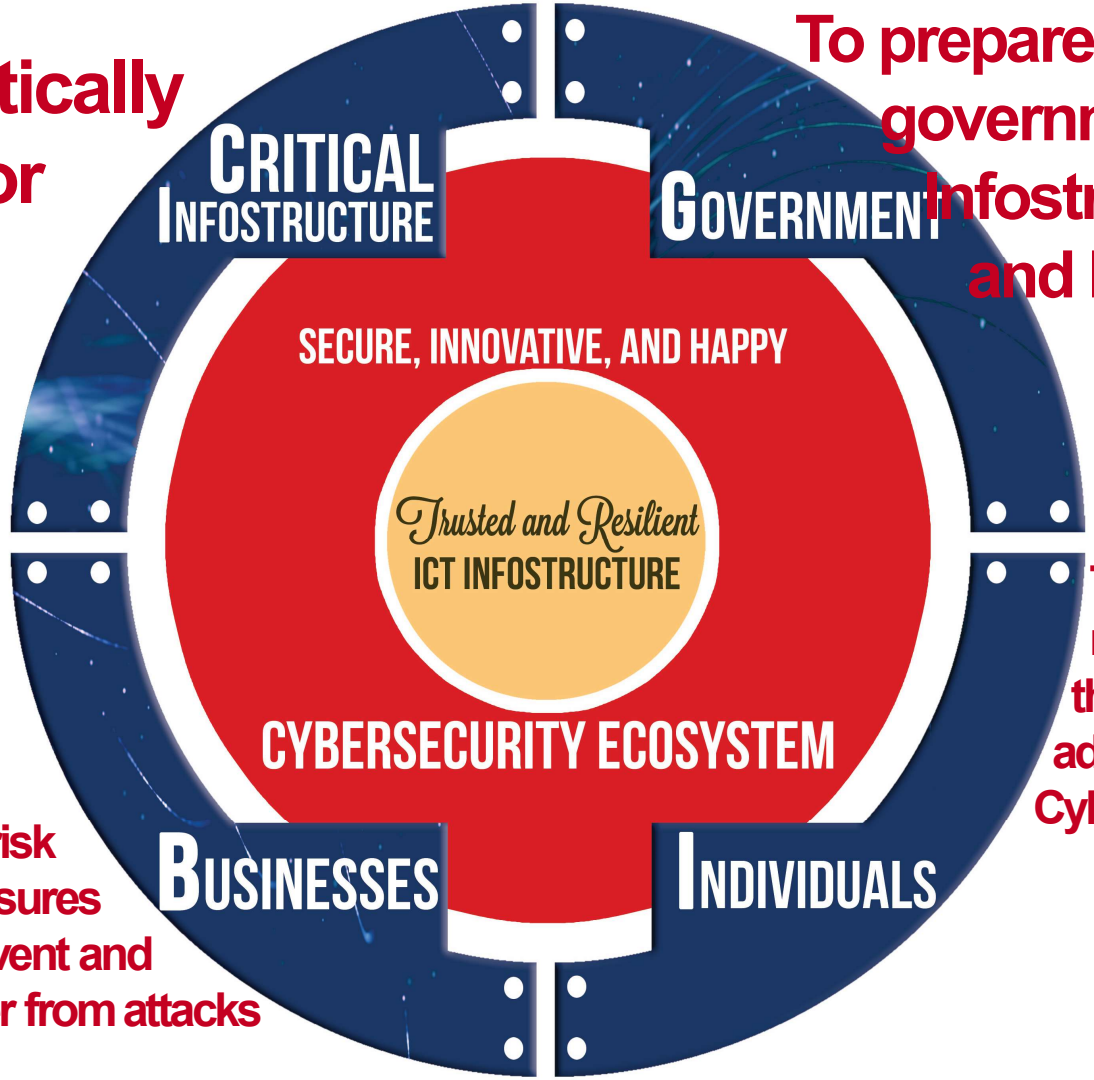


#CyberSafePH

Making Individuals Aware and Secure

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

To systematically harden CII for Resiliency



To prepare and secure government ICT Infostructure (Public and Military)

To raise awareness on cyber risks among users as they are the weakest links, they need to adopt the right norms in CyberSecurity

To raise awareness of cyber risk and use of security measures among businesses to prevent and protect, respond and recover from attacks

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

Key Strategic Imperatives

Protection of Critical Infostructure (CII)

CyberSecurity Assessment and Compliance Programs

Public Networks thru establishment of CERTs

Military Networks thru establishment of Cyber Defense Centers (DND, NSC, AFP)

Protection of Government Networks (Public and Military)

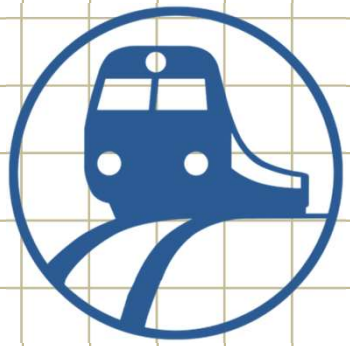
Protection of Businesses and Supply Chains

National Common Criteria Evaluation and Certification Program

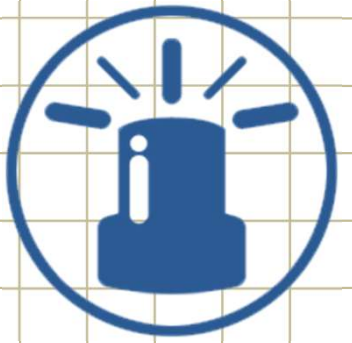
CyberSecurity Education Campaign Program

Protection of Individuals

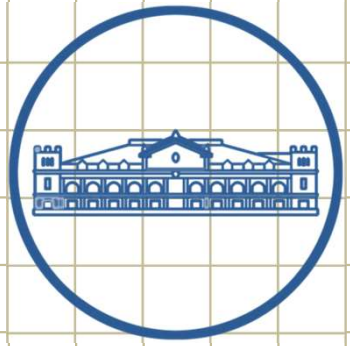
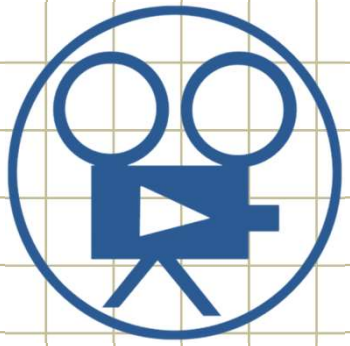
DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY



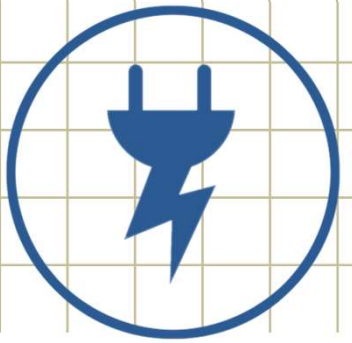



Critical Infostructure





DICT Cybersecurity Bureau
ACCOMPLISHMENTS

Publication of the National CyberSecurity Plan 2022 (NCSP 2022)

- Launched on December 8, 2016
- Various roundtable discussions / consultations with vital sectors were done
- Published on May 2, 2017
- Available for download at www.dict.gov.ph

ISSUANCE OF **MEMORANDUM CIRCULARS**

Implementation of the **NCSP 2022**

Protection of Critical Infostructure **(DICT-MC 005)**

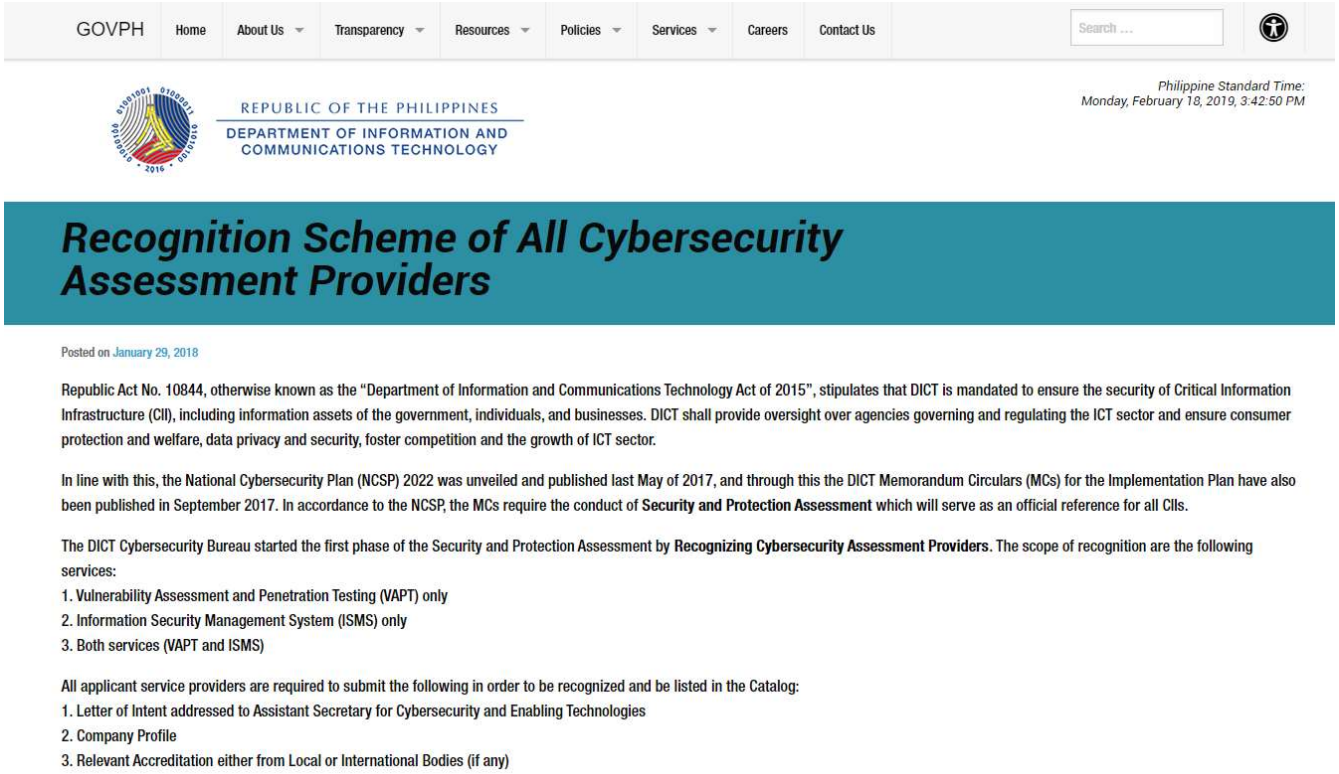
Protection of Government Agencies **(DICT-MC 006)**

Protection of Individuals **(DICT-MC 007)**

The **MCs** state the general policies of the state in cybersecurity and directs relevant agencies and companies to comply.

DICT SECURITY **ASSESSMENT RECOGNITION SCHEME**

Implementation of the **NCSP 2022**



GOVPH | Home | About Us | Transparency | Resources | Policies | Services | Careers | Contact Us | Search ...

REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

Philippine Standard Time:
Monday, February 18, 2019, 3:42:50 PM

Recognition Scheme of All Cybersecurity Assessment Providers

Posted on January 29, 2018

Republic Act No. 10844, otherwise known as the "Department of Information and Communications Technology Act of 2015", stipulates that DICT is mandated to ensure the security of Critical Information Infrastructure (CII), including information assets of the government, individuals, and businesses. DICT shall provide oversight over agencies governing and regulating the ICT sector and ensure consumer protection and welfare, data privacy and security, foster competition and the growth of ICT sector.

In line with this, the National Cybersecurity Plan (NCSP) 2022 was unveiled and published last May of 2017, and through this the DICT Memorandum Circulars (MCs) for the Implementation Plan have also been published in September 2017. In accordance to the NCSP, the MCs require the conduct of **Security and Protection Assessment** which will serve as an official reference for all CIIs.

The DICT Cybersecurity Bureau started the first phase of the Security and Protection Assessment by **Recognizing Cybersecurity Assessment Providers**. The scope of recognition are the following services:

1. Vulnerability Assessment and Penetration Testing (VAPT) only
2. Information Security Management System (ISMS) only
3. Both services (VAPT and ISMS)

All applicant service providers are required to submit the following in order to be recognized and be listed in the Catalog:

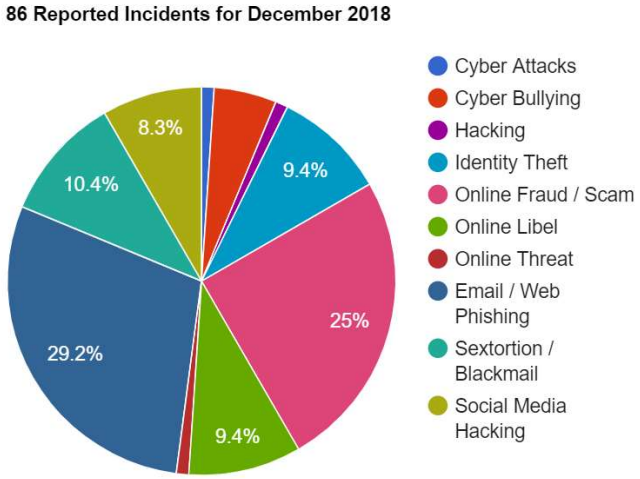
1. Letter of Intent addressed to Assistant Secretary for Cybersecurity and Enabling Technologies
2. Company Profile
3. Relevant Accreditation either from Local or International Bodies (if any)

http://dict.gov.ph/recognition-scheme-cybersecurity-assessment-providers/

- DICT CyberSecurity Bureau Conducts VAPT for government Agencies
- For government agencies and other CIIs who prefer private companies to do the VAPT, the Bureau has a Recognition Scheme for all Cybersecurity Assessment Providers

NATIONAL COMPUTER EMERGENCY RESPONSE TEAM **(NCERT)** WEBSITE

Implementation of the **NCSP 2022**

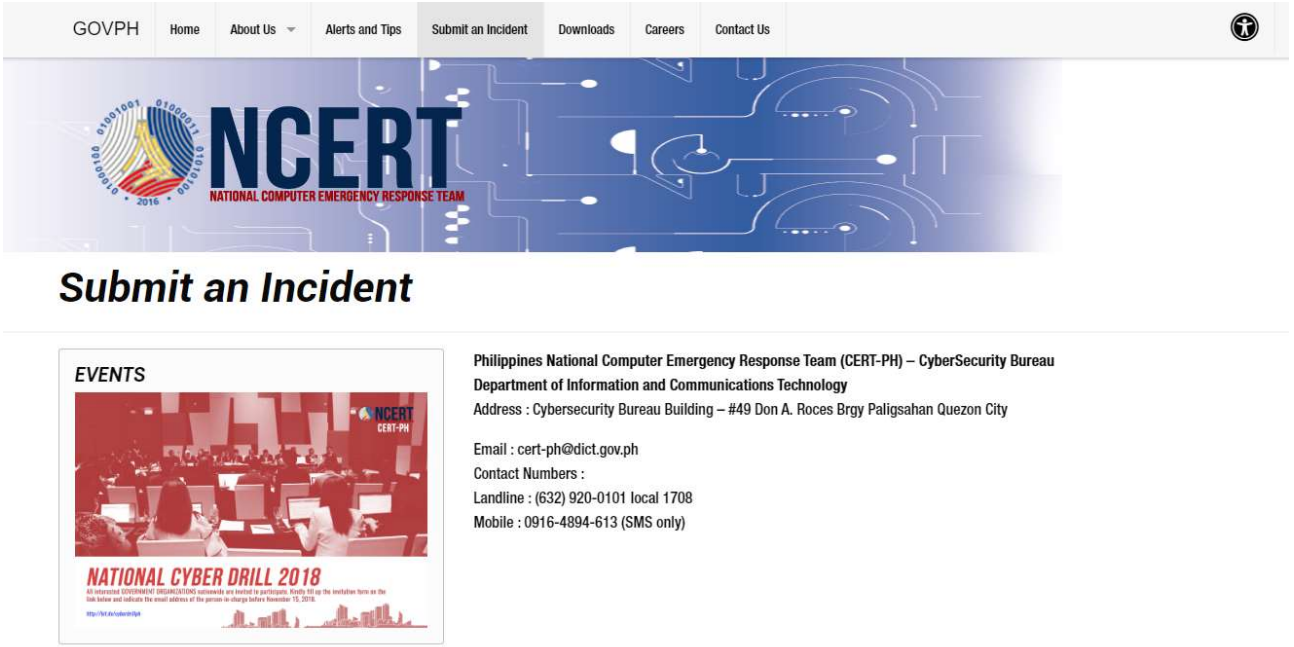


https://www.ncert.gov.ph/

- **Status:** Launched at the Philippine Cybersecurity Conference 2018
- This is an informative website focusing on threat and vulnerability warnings and alerts. It has an embedded Helpdesk Ticketing System that shareholders can use in reporting cyber attacks and cybercrimes.

INCIDENT REPORT STATISTICS SYSTEM

Implementation of the **NCSP 2022**



https://www.ncert.gov.ph/submit-an-incident/

- **Status:** 100%
- It is a web application that is used to collect data and transform information and incidents reported to the Cybercrime Investigation and Coordination Center (CICC) into statistics pies.

CREATION OF **SECTORAL CERTS**

Implementation of the **NCSP 2022**

COMPUTER EMERGENCY RESPONSE TEAM (CERT) MANUAL

The draft of the CERT Manual has been disseminated to CIIs and government agencies for inputs.

ENGAGEMENT WITH CRITICAL INFOSTRUCTURE (CIIS)

- Focus Group Discussions with the Identified CIIs
- CyberSecurity Strategy Consultation Military – National Military Strategy
- DOE CyberSecurity Policy Writeshop

CYBERSECURITY AWARENESS & **INFORMATION CAMPAIGN**

Implementation of the **NCSP 2022**

Universidad de Zamboanga
Zamboanga City
April 21, 2017
Attendees: 1200

AMA Computer University
Quezon City
July 21, 2017
Attendees: 1200

Ateneo de Davao University
Davao City
July 28, 2017
Attendees: 1000

University of Science and Technology of Southern Philippines
Cagayan de Oro City
August 10, 2017
Attendees: 3000

Laguna State Polytechnic University, San Pablo City
September 22, 2017
Attendees: 2000

Silliman University
Dumaguete City
November 10, 2017
Attendees: 1200

University of San Carlos
Cebu City
December 18, 2017
Attendees: 250

Emiliana Hall, Balanga City, Bataan
January 19, 2018
Attendees: 1000

Sweet Harmony Gardens
Taytay Rizal
January 26, 2018
Attendees: 2000

Rizal Triangle Multi-Purpose Gym, Olongapo, Zambales
June 29, 2018
Attendees: 700

The main cybersecurity awareness program of the DICT is the Cybersecurity Awareness & Information Campaign conducted in various schools nationwide.

Catanduanes State University, Catanduanes
July 1, 2018
Attendees: 700

Bicol University, Legazpi
July 19, 2018
Attendees: 2200

Ateneo de Naga University, Naga City, Camarines Sur
July 20, 2018
Attendees: 500

University of Southeastern Philippines, Davao City
October 24, 2018
Attendees: 100

Mindanao State University Bongao City, Tawi-Tawi
November 29, 2018
Attendees: 1124

Western Mindanao State University, Zamboanga City
December 1, 2018
Attendees: 1072

University of Southern Mindanao, Kidpawan City
February 7, 2019
Attendees: 1000

INTEGRATION OF THE **CYBERSECURITY CURRICULUM** TO THE PH EDUCATION SYSTEM

Implementation of the **NCSP 2022**

AMA Computer University
Bachelor of Science in CyberSecurity

Holy Angel University (Pampanga)
Professional Science Masters (PSM) in CyberSecurity

- Partnership with the Commission on Higher Education to develop a cybersecurity curriculum tailor-fit for the Philippines
- Meeting with school administrators all over the Country

CHILD **ONLINE PROTECTION**

Implementation of the **NCSP 2022**

Anti- Online Sexual Exploitation of Children

Anti- Cyberbullying

Digital Parenting

- Anti-Cyberbullying video competition for high school & college students
- Focus Group Discussion on Anti-Online Sexual Exploitation of Children
- Digital Parenting Conference

RULE ON **CYBERCRIME WARRANTS**

DICT Cybersecurity Bureau was part of the Technical Working Group that developed the Rule on Cybercrime Warrants

Implementation
of the **NCSP 2022**

END OF PRESENTATION

THE PHILIPPINES'

CYBERSECURITY LAWS, BEST PRACTICES, AND STRATEGIES

Cybersecurity Bureau | *cybersecurity@dict.gov.ph*
(02) 920 0101 local 1002

@CYBERSECgovph