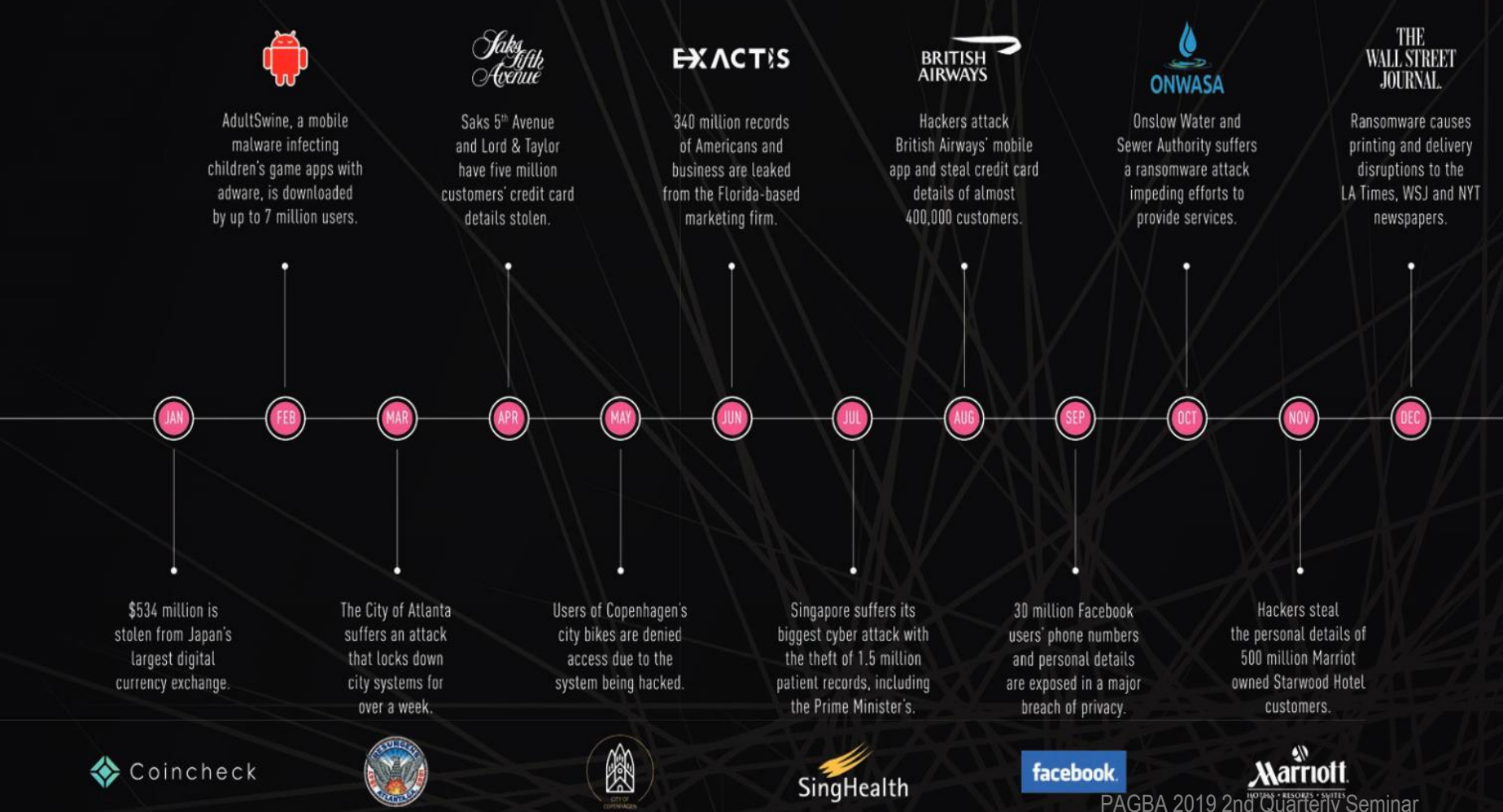
National CyberSecurity Plan 2022

Allan S. Cabanlong, ASEAN Engr.
Assistant Secretary
Cybersecurity and Enabling Technologies

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY


RECENT
CYBER
THREATS


AdultSwine, a mobile malware infecting children's game apps with adware, is downloaded by up to 7 million users.
Saks 5th Avenue and Lord & Taylor have five million customers' credit card details stolen.
340 million records of Americans and business are leaked from the Florida-based marketing firm.
Hackers attack British Airways' mobile app and steal credit card details of almost 400,000 customers.
Onslow Water and Sewer Authority suffers a ransomware attack impeding efforts to provide services.
Ransomware causes printing and delivery disruptions to the LA Times, WSJ and NYT newspapers.
JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC
$534 million is stolen from Japan's largest digital currency exchange.
The City of Atlanta suffers an attack that locks down city systems for over a week.
Users of Copenhagen's city bikes are denied access due to the system being hacked.
Singapore suffers its biggest cyber attack with the theft of 1.5 million patient records, including the Prime Minister's.
30 million Facebook users' phone numbers and personal details are exposed in a major breach of privacy.
Hackers steal the personal details of 500 million Marriot owned Starwood Hotel customers.
Coincheck
SingHealth
facebook
Marriott

Attacks to CII

Bank Heist, **N**avigation Systems Manipulation,
Control of Electronic Medical Equipment and Records,
Override of Oil and Gas Systems

Attacks to Government Infostructure

Hacking resulting in Data breach
Defacement of PH Government Agencies Websites

Sophistication of Cyber Attacks

APT, **D**DoS, **S**PAM, **S**pear Phishing,
Social Engineering

12-pt National Security Goals

- 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

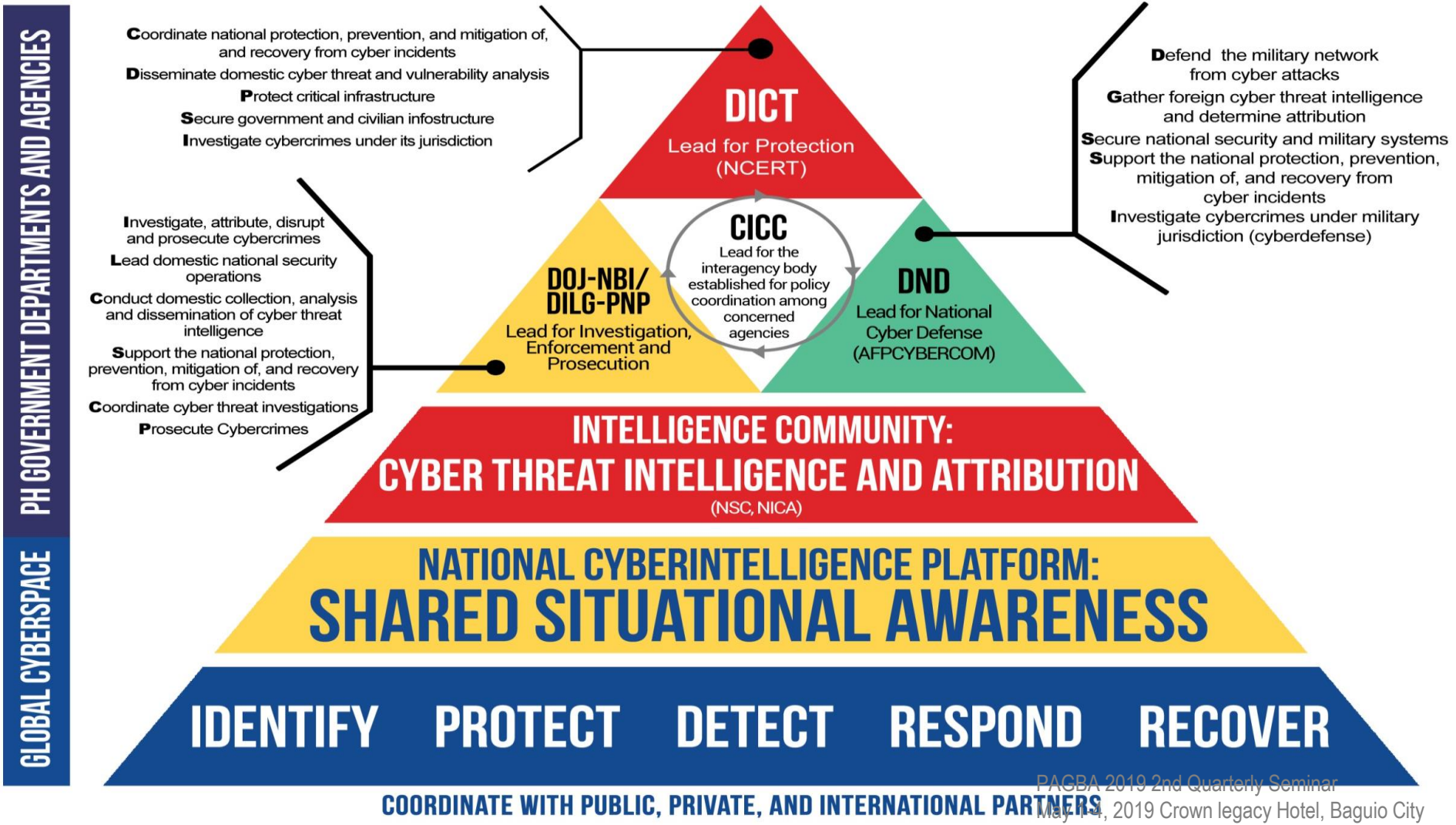
National Security Strategy

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

2018

PAGBA 2019 2nd Quarterly Seminar
May 1-4, 2019 Crown legacy Hotel, Baguio City

NATIONAL CYBERSECURITY PLAN 2022


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)
CICC
Lead for the interagency body established for policy coordination among concerned agencies
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
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

Key Strategic Imperatives

Public Networks thru establishment of CERTs

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

CyberSecurity Education Campaign Program

Protection of Critical Infostructure (CII)

Protection of Government Networks (Public and Military)

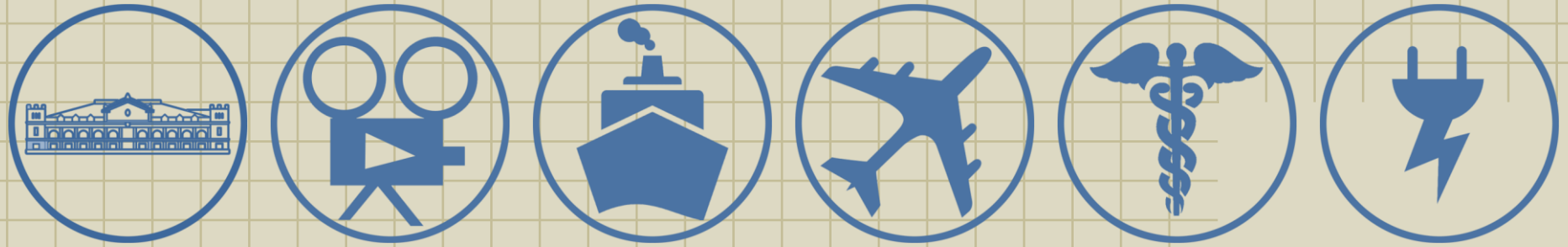
Protection of Businesses and Supply Chains

Protection of Individuals

CyberSecurity Assessment and Compliance Programs

National Common Criteria Evaluation and Certification Program

Critical Infostructure



National CyberSecurity Plan Implementation Milestones

PAGBA 2019 2nd Quarterly Seminar
May 1-4, 2019 Crown legacy Hotel, Baguio City

Memorandum Circulars 005 to 007, s2017

Issuance of Memorandum Circulars (MC) on the following:

- **Protection of Critical Infostructure (DICT-MC 005);**
- **Protection of Government Agencies (DICT-MC 006; and**
- **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
- The MCs can be downloaded at www.dict.gov.ph

DICT Security Assessment Recognition Scheme

- 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

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, March 12, 2018, 10:51:33 AM

Recognition Scheme of All Cybersecurity Assessment Providers

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:

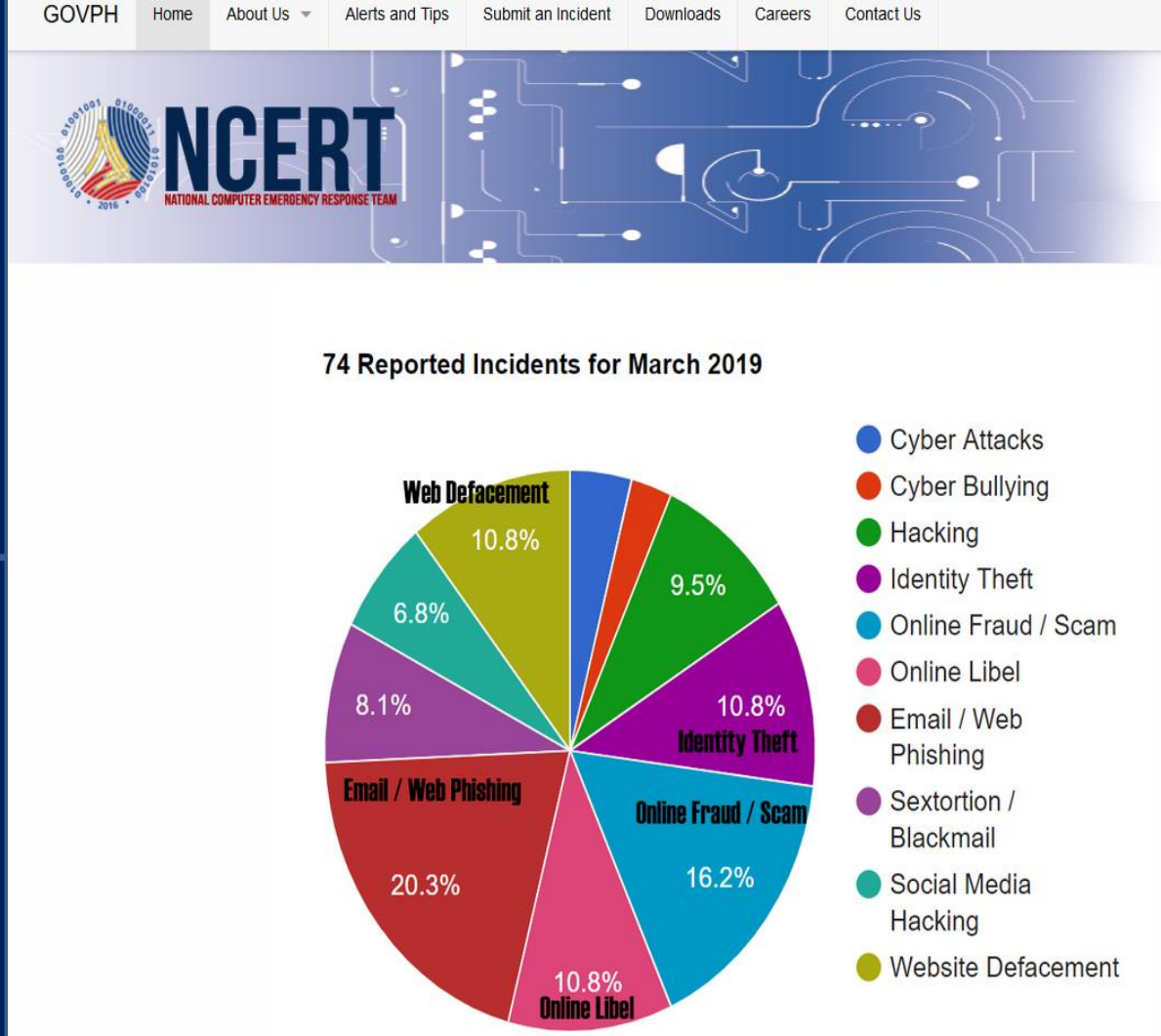
1. Letter of Intent addressed to Assistant Secretary for Cybersecurity and Enabling Technologies
2. Company Profile
3. Relevant Accreditation either from Local or International Bodies (if any)

National Computer Emergency Response Team Website
(NCERT Website)

- **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

- **Status: 100% working**
- **It is a web application that is used to collect data and transform information and incidents reported to CERT-PH into usable statistics**



Critical Infostructure FGDs

Computer Emergency Response Team (CERT) Manual

- The draft of the Computer Emergency Response Team (CERT) Manual has been disseminated to CIIs and government agencies for inputs.

Engagements with Government and CIIs on the creation of Government and Sectoral CERTs

- FGD with the Energy Sector representatives – Oct. 23, 2017
- Meeting with the Military Sector/AFP – Nov. 8, 2017
- FGD with Energy Sector - April 18, 2018
- FGD with Banking and Finance Sector - May 21, 2018
- DOE Cybersecurity Policy Writeshop – June 13-14, 2018
- FGD with BPO and Health Sectors- June 26, 2018
- FGD with transportation, Water, Utilities, and Emergency Services Sectors – August 3, 2018

Energy Sectoral CERT

What has been done?

- FGD with the Energy Sector resulting in identification of the Department of Energy (DOE) as lead for the Energy Sectoral CERT
- CyberSecurity Policy Writeshop with DOE
- CERT Training for DOE IT personnel

What's next?

- Establishment of the National Energy Cybersecurity Governance Framework
- National CyberSecurity Strategy for the Energy Sector
- DOE's Cyber Resilience Network Infrastructure (CRNI)

Capacity Building Initiatives

CERT Training

Course 001: CERT Training – May 22-23, 2018
- 45 Participants (DICT Clusters and IT officers of Priority Agencies)

Course 001: CERT Training – August 31, 2018
- 50 Participants (IT and Policy officers of Priority Different Agencies)

CYBERSECURITY AWARENESS & INFORMATION CAMPAIGN

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

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

Ateneo de Davao Universit
y 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

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
December 1, 2018
Attendees: 1072

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

Iligan State University
Iligan, Cagayan de Oro
April 5, 2019

Isabela State University
Echague, Isabela
April 10, 2019

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

Integration of Cybersecurity in the Academe

Campaign to integrate CyberSecurity into the Philippine education system

- 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
- Through this advocacy, the following have pioneered the offering of the following in their respective universities:

AMA Computer University

Bachelor of Science in CyberSecurity

Holy Angel University (Pampanga)

Professional Science Masters (PSM) in CyberSecurity

Protection of the most vulnerable sector of the society

Child Online Protection

- Anti- Cyberbullying
- Anti- Online Sexual Exploitation of Children
- Digital Parenting

- Launch of the Anti-Cyberbullying video competition for high school & college students | Jul 9, 2018
- FGD on Digital Parenting | August 5, 2018
- Focus Group Discussion on Anti-Online Sexual Exploitation of Children | Aug 8, 2018
- Digital Parenting Conference for DICT | Aug 25, 2018
- Child Online Protection Stakeholders Consultation | September 28, 2018
- Regional Digital Parenting Campaign 2019 conducted in Cagayan de Oro, Isabela, and Davao City

Rule on Cybercrime Warrants

DICT CyberSecurity Bureau served as Subject Matter Expert (SME) in the development of the RCW which took effect August 15, 2018.

International Cooperation

The Philippines became the 57th party to the Budapest Convention after the Senate unanimously concurred on the signing of the instrument of accession in February 2018.

The Philippines endorsed the Paris Call for Trust and Security in Cyberspace in November 2018.

The Philippines actively and strongly supports ASEAN initiatives towards norms and legal frameworks in the region.

The Cybersecurity Management System Project (CMSP)

REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

PAGBA 2019 2nd Quarterly Seminar
May 1-4, 2019 Crown legacy Hotel, Baguio City

CMSP

The Cybersecurity Management System Project is a national platform for intelligence sharing to comprehensively monitor threats and defend the country's infostructure from ever-increasing cyber threats and cyber-attacks.

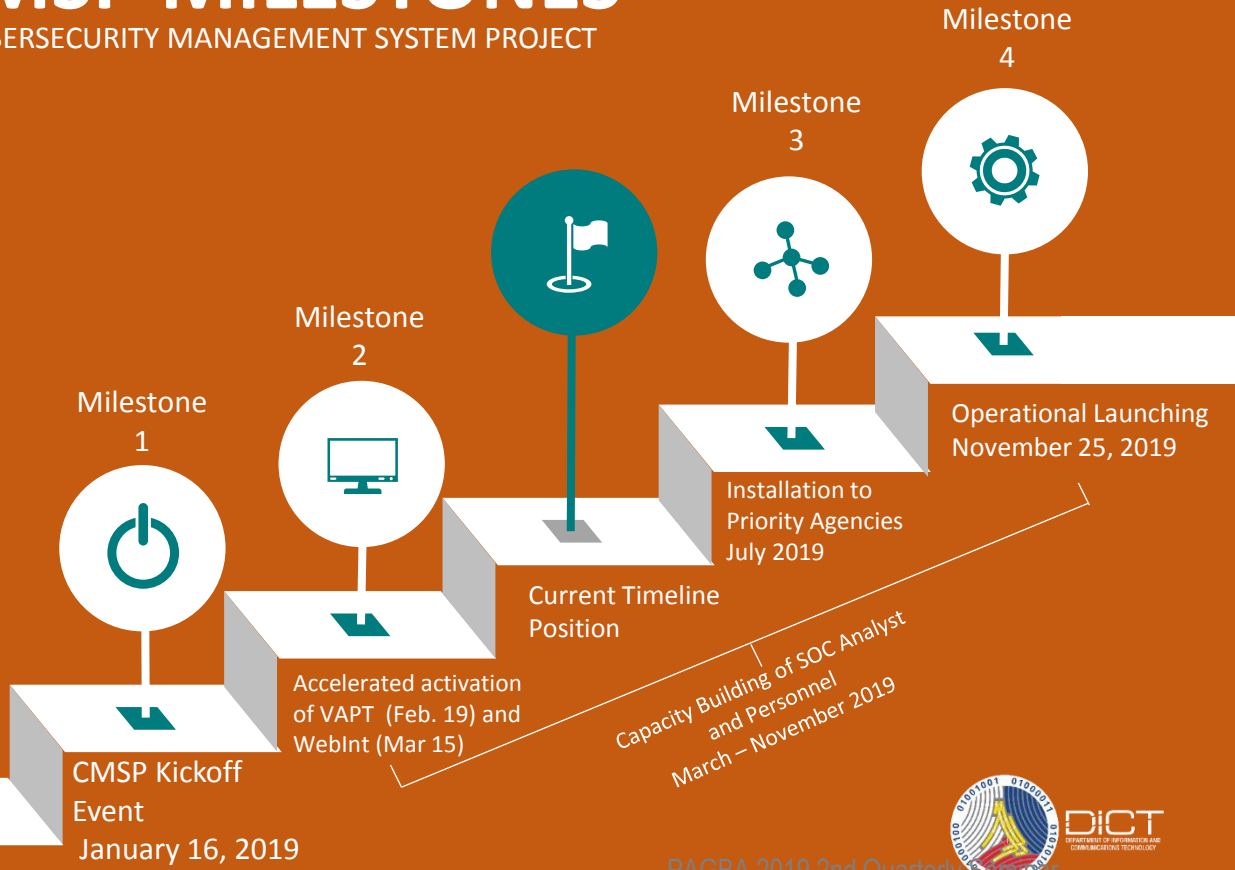
PAGBA 2019 2nd Quarterly Seminar
May 1-4, 2019 Crown legacy Hotel, Baguio City

CMSP MILESTONES

CYBERSECURITY MANAGEMENT SYSTEM PROJECT

CURRENT TIMELINE POSITION

Wrapping-up stage on the build-up of the Security Operations Center (SOC). Currently the vulnerability assessment penetration test (VAPT) tool component of the CMSP has been activated, up and running. Ongoing review and finalization of Memorandum of Agreement (MOA) for priority agencies for CMSP. To date, three (3) confirmed top priority agencies are OP-Proper, DICT and DND.



The Cybersecurity Bureau

Cybersecurity Management System Project

The construction of the Security Operation Center of the Cybersecurity Bureau now on the finishing stage on the civil works and final configuration and tune-up of the hardware and software.

THE DOLL

CYBERCRIME SITUATION IN THE PHILS

INDEPENDENT

JOIN US SUBSCRIBE / REGISTER LOGIN

NEWS POLITICS VOICES FINAL SAY SPORT CULTURE VIDEO INDY/LIFE INDYBEST LONG READS INDY100

News > UK > Crime

Child sex abuse live streams rising at 'alarming rate' amid surge in 'cybersex trafficking'

'Dark' form of exploitation sees children perform sex acts online for paedophiles in UK

QUARTZ

OBSESSIONS | EMAILS | EDITIONS

POPULAR | LATEST | FEATURED

Unicef calls the Philippines the "global epicenter" of live-streamed child pornography

CONCEPT CENTRAL

ALL THE NEWS THAT MATTERS

HOME TOP STORY NATION WORLD SPORTS BUSINESS EDITORIAL OPINION MORE

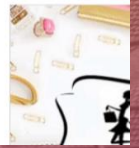
Home › Headlines › Phl is online child sex capital of the world, warns UNICEF

Headlines Latest News Nation Top Story

Phl is online child sex capital of the world, warns UNICEF

June 7, 2016 2:25 PM

227



The Economist

Topics Current edition More

Caught in the web

The Philippines is a global hub for child pornography

Police are experimenting with new methods to catch online buyers

RAPPLER

News Video Business Newsbreak MovePH Views Life & Style Entertainment Sports Tech

PHILIPPINES

Philippines top global source of child pornography – Unicef

8 out of 10 Filipino children at risk of online sexual abuse or bullying

Patty Pasion

@pattypasion

Published 11:58 AM, December 13, 2017

Updated 11:58 AM, December 13, 2017

Facebook

ONE VOICE AGAINST MODERN SLAVERY

FREEDOMUNITED

Learn Act Give

Back to Global News

THOMSON REUTERS FOUNDATION Monday March 26, 2018

Philippines: 3,000 Reports Each Month of Child Cybersex Abuse

0 Child Slavery, Human Trafficking, Prevention

CyberSafePH

ECO-SYSTEM ACTIVATION & PLANNING WORKSHOP

MARCH 7-8, 2019

PAGBA 2019 2nd Quarterly Seminar
May 1-4, 2019 Crown legacy Hotel, Baguio City

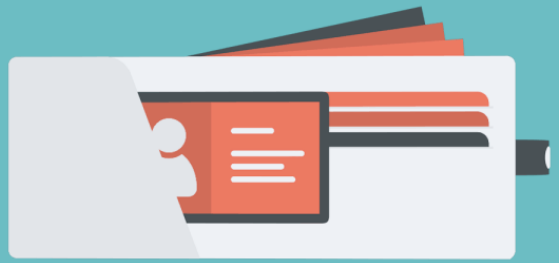
NATIONAL ID SYSTEM

PAGBA 2019 2nd Quarterly Seminar
May 1-4, 2019 Crown legacy Hotel, Baguio City

RA 11055 – Philippine Identification Systems Act

Section 18 of R.A. 11055,

"The Philippine Statistics Authority (PSA) with the technical assistance from the **DICT shall implement** reasonable and appropriate, organizational, **technical and physical security** measures to ensure that the information gathered by PhilSys, is protected by **unauthorized access, use disclosure, and against accidental or intentional loss, destruction or damaged.**



Cybersecurity Takeaways

Always secure your digital assets from cyberattacks. The increasing pace of the possibilities provided by the internet services has become an aide for businesses and opportunities to maximize the use of the internet. Our ICT assets rely heavily on the use of the internet, the same field where hackers and cyber criminals rely on the to enact their illicit deeds. As convenient and helpful the internet has been to each individual, we do not realize the implications of a cyber attack unless we've been struck by one. The implications and consequences and consequences of poorly implemented systems and the ignorance of understanding the risks posed on the ICT assets can lead to immense financial and reputational loss.

- January 2019

Cybersecurity: Be A Part of It

Report an incident by contacting:

THE PHILIPPINE NATIONAL CYBERSECURITY EMERGENCY RESPONSE TEAM (CERT)

Landline Phone: (02) 920-0101 local 1002 and 1708
Mobile : 0916-489-4613
Email: cert-ph@dict.gov.ph
Social Media: fb.com/ncertgovph

Thank You!

REPUBLIC OF THE PHILIPPINES

DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY