Republic of the Philippines
Department of Information and Communications Technology (DICT)

National Cybersecurity Plan 2023-2028

February, 2024.

Rights and permissions

The DICT does not claim that all the ideas presented here were exclusive and original. The NCSP 2023-2028 is a product of a collective effort incorporating ideas and works from various government agencies and organizations voluntarily submitted to the DICT through official correspondences.

February, 2024

Message from the President

Amidst the accelerating tempo of technology progress and a vastly interconnected global landscape, the Philippines emerges as a pivotal player with a capacity to transform into a digitally advanced nation. But in order to fully realize these developments, it is imperative that we also give our utmost attention to its many accompanying challenges.

Guided by strong developmental principles, the National Cybersecurity Plan 2024-2029 of the Department of Information and Communications Technology aims to position the country at the cutting edge of the digital age. By reinforcing our cybersecurity defense strategies, we prepare ourselves for the imminent risks that come with these new advancements.

As we look towards the future, I urge all government agencies, the private sector, and citizens to continue to work together in creating a secure digital environment for everyone. United as one, let us place trust, accountability, and transparency at the forefront of our collective endeavors so that we can move forward with courage and determination as we shape the future and leave a lasting impact on the work stage.

Together, let us make the Philippines rise to its fullest potential.

FERDINAND R. MARCOS, JR.
President
Republic of the Philippines

Message from the Secretary

During and after the COVID-19 pandemic, a steady increase in internet-based transactions were observed. Electronic commerce and e-banking became a norm, and the country steadily moved to cashless transactions, driven mostly by innovations from the private sector. As these developed, cybercrime incidents also increased. Threat actors in cyberspace exploited weaknesses and vulnerabilities both in the technology, processes, and human behavior. The National Cybersecurity Plan 2024-2029 (NCSP 2023-2028) is a response to these developments. Our mission is *to ensure a trusted, secure, and reliable cyberspace for every Filipino*. This reflects the need to defend government and our people in cyberspace, and a recognition of the importance of building trust in cyberspace which is necessary for economic growth.

The second iteration of the NCSP was built upon the successes of the previous strategy, yet also demonstrates a shift in policy. We now aim to pass a Cybersecurity Law that seeks to balance the economic relationships affecting non-compliance to cybersecurity regulations. The new strategy also favors standards-based policy and risk-based approaches. Individual organizations, instead of entire sectors, are identified as a CII, should they fail, based on their size and impact. A renewed focus on building the cyber-workforce and the importance of enhancing international cooperation for cybersecurity was also reiterated.

Most importantly, the NCSP 2023-2028 shows the importance of convergence among all government agencies in delivering our mission. It outlines steps on how each government agency can coordinate all their cybersecurity initiatives through the National Cybersecurity Inter-Agency Committee (NCIAC). It also harmonizes all organization CERT and defined two national-level CERTs.

Admittedly, the NCSP 2023-2028 is ambitious. With the help of all government agencies, the private sector, and all branches of government, we believe this strategy is doable.

ATTY. IVAN JOHN E. UY
Secretary
DICT

Preface

Under Section 15 of RA 10844, DICT has the mandate to develop the National Cybersecurity Plan (NCSP) and to lead the national effort for cybersecurity. The NCSP 2023-2028 is the second iteration of the NCSP and improves on the foundation of the previous plan. The NCSP 2023-2028 is a product of meaningful consultations between different stakeholders both from the public and the private sectors. Prior to the release of the public draft, the DICT has conducted more than twenty small pocket consultations with different organizations. The publication of the public draft of the NCSP 2023-2028 last May 2023 generated interest and discussions. Three large public consultations were conducted using the public draft. More than thirty (30) position papers and numerous comments and suggestions from different stakeholders were submitted to DICT. Most of these comments were incorporated in this final version of the plan. The DICT, led by Secretary Ivan John E. Uy, thanks all the participants and commenters. Gratitude is also extended to the Private Sector Advisory Council (PSAC) that assisted in facilitating most of these public consultations and to the Presidential Management Staff who organized many of the inter-agency consultations.

The plan is ambitious and reflects the goal of the administration of His Excellency Ferdinand "Bongbong" R. Marcos, Jr. to bring the Philippines at the forefront of the digital era safely and securely. As e-Commerce and digital transactions in government grow, the pressure to defend information assets in cyberspace also rises. This plan presents a clear roadmap on how the rights of citizens and the nation can be protected in cyberspace.

The NCSP is consistent with the Philippine Development Plan 2023-2028, the National Security Strategy, the National Cybercrime Strategy and other strategies developed by other national government agencies that either share or have similar mandates in cybersecurity.

JEFFREY IAN C. DY
Undersecretary
Infostructure Management,
Cybersecurity, and Upskilling

Table of contents

List of acronyms

AFP	Armed Forces of the Philippines
AI	Artificial Intelligence
AS	Autonomous System
ASN	Autonomous System Numbers
BGP	Border Gateway Protocol
BPO	Business Process Outsourcing
CERT	Computer Emergency Response Team
CGNAT	Carrier Grade Network Address Translation
CHED	Commission on Higher Education
CI	Critical Infrastructure
CIA	Confidentiality, Integrity, Availability (aka the CIA Triad)
CIANA-PS	Confidentiality, Integrity, Availability, Non-Repudiation, Authentication, Privacy Safety
CICC	Cybercrime Investigation and Coordinating Center
CII	Critical Information Infrastructure
CPE	Customer Premise Equipment
CSB	Cybersecurity Bureau of the DICT
CSC	Civil Service Commission
CSE	Career Service Eligibility
CSV	Comma Separated Value
CVSS	Common Vulnerability Scoring System
DFA	Department of Foreign Affairs
DICT	Department of Information and Communications Technology
DND	Department of National Defense
DOJ	Department of Justice
DTI	Department of Trade and Industry
EU	European Union
GCI	Global Cybersecurity Index

GDP	Gross Domestic Product
GDPR	General Data Protection Regulation (of the European Union)
GOCC	Government Owned and Controlled Corporation
ICT	Information and Communications Technology
IDS	Intrusion Prevention System
ILCDB	ICT Literacy and Competency Development Bureau of the DICT
InterPol	International Criminal Police Organization
IOT	Internet of Things
IPS	Intrusion Protection System
IS	Information System or Information Service
ISO	International Organization for Standardization
ISP	Internet Service Providers
ITU	International Telecommunications Union
LGU	Local Government Units
NBI	National Bureau of Investigation
NBP	National Broadband Program
NCERT	National Computer Emergency Response Team
NCIAC	National Cybersecurity Inter-Agency Committee
NCIN	National Cyber Intelligence Network
NCS	National Cybercrime Strategy
NCSP	National Cybersecurity Plan
NGA	National Government Agency
NGDC	National Government Data Center Project
NICA	National Intelligence Coordinating Council
NSC	National Security Council
NTC	National Telecommunications Commission
OECD	Organization for Economic Cooperation and Development
PCG	Philippine Coast Guard

PDP	Philippine Development Plan
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PNP	Philippine National Police
PSA	Philippine Statistics Authority
PTE	Public Telecommunication Entities
RA	Republic Act
S-BGP	Secure Border Gateway Protocol
SDNS	Secure DNS
Socmed	Social Media
SSL	Secure Socket Layer
TESDA	Technical Education and Skills Development Authority
TLS	Transport Layer Security
TTP	Tactics, Techniques, and Procedures
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
VAPT	Vulnerability Assessment and Penetration Testing
WAN	Wide Area Network

Definition of terms

The following are the definitions of terms used in this document. Most are defined using the ISO 27000 family of standards especially [1] and [2]. The term cyber attribution is defined using the paper by Saalbach published March 2019 [3]

Asset

Anything that has value to an individual, an organization, or a government.

Authenticity

Property that an entity is what it claims to be.

Availability

Property of being accessible and usable upon demand by an authorized entity.

CERT-PH

The official name of the Philippine National CERT (NCERT)

Confidentiality

Property that information is not made available or disclosed to unauthorized individuals, entities, or processes

Critical Information Infrastructure

Consists of information process and Information Communications Technology which form part of the operation of the Critical Infrastructures (CI).

Critical Infrastructures

A set of systems and assets that are essential to a nation such that any disruption of their service can have a serious impact on national security, economy, social well-being, and citizen safety.

Cyber Attribution

Tracing the perpetrators of a cyber attack to a certain attacker or a group of attackers, and then unveiling the real-world identity of the attacker.

Cybersecurity

The organization and collection of resources, processes, and structures to preserve Confidentiality, Integrity, Availability, Non-Repudiation, Authenticity, Privacy and Safety (CIANA-PS) in cyberspace.

Cybersecurity Incident (interchangeably information security incident)

A single or series of unwanted or unexpected information security (cybersecurity) events that have a significant probability of compromising business operations and threatening information security (cybersecurity).

Cyberspace

A complex environment emerging from the interaction of people, software, and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form.

Integrity	Property of accuracy and completeness.
Non Repudiation	Ability to prove the occurrence of a claimed event or action and its originating entities.
Privacy	Having the personal control over personal information.
Reliability	Property of consistent intended behavior and results.
Risk	The potential loss of confidentiality, integrity, or availability of information, data or information systems and reflects the potential adverse impacts to organizational operations, assets, individuals, other organizations, and the nation.
Threat	Potential cause of an unwanted incident, which may result in harm to a system, individual, or organization.
Vulnerability	Weakness of an asset or control that can be exploited by one or more threats.

Context of the NCSP 2023-2028

Mandate and scope

Republic Act 10844 mandated the Department of Information and Communications Technology or the DICT to formulate and implement the National Cybersecurity Plan (NCSP) [4][1]. The first iteration of the plan was published in 2017 and was in force from 2017 to 2022. This laid the foundation for much of the Department's work in cybersecurity. Through the NCSP 2017-2022, the National CERT was organized, and a reporting mechanism was established. However, efficiently responding to cybersecurity incidents still requires improvement, and there is much work that needs to be done in protecting our CIIs. Thus, under the new administration of President Ferdinand "Bongbong" Marcos Jr. (PBBM) and amid the exponential growth in cybersecurity incidents, the NCSP 2023-2028 is formulated.

The DICT shall be the lead agency in implementing the NCSP 2023-2028. While cybersecurity requires a whole-of-nation and multi-disciplinary approach, all government agencies, including LGUs, are encouraged to develop and improve their own cybersecurity strategies and sub-plans that are consistent with the NCSP 2023-2028. All government agencies are also enjoined to create their own cybersecurity teams to significantly improve each agencies' cybersecurity posture.

NCSP 2023-2028 as a sub-plan of PDP 2023-2028

The PDP 2023-2028, as the national development blueprint, reflects the socio-economic agenda of PBBM and regards cybersecurity as critical, not only to peace and security but also to economic development. It aims to improve e-Commerce and digital trade by strengthening regulatory frameworks in the areas of transparency, privacy, and cybersecurity [5]. The NCSP 2023-2028 is a sub-plan of the PDP 2023-2028, which pertains to cybersecurity. The different strategic objectives in the PDP, in line with cybersecurity, are outlined below.

- ◉ Chapter 7: Transform production sectors to generate more quality jobs and competitive products.
    - ➡ Outcome 1: Market Expansion Achieved.
        - ‣ Ensure the safety and security in the cyber and physical spaces strategy discusses the necessity of cybersecurity and outlines the passing of the Cybersecurity and the Critical Information Infrastructure Protection Law/s as essential components of a strengthened legal framework for cybersecurity.
        - ‣ Accelerate e-commerce adoption by micro, small, and medium enterprises strategy mentions the promotion of a cybersecurity culture in both global and local context as essential to achieving the strategy.
        - ‣ Spearhead active promotions of tourism, culture, creative industries, and information technology and business process management strategy

[1] RA 10844 (2015) Section 15.3.b.i transferred cybersecurity functions, including the creation of the NCSP, and establishment of the NCERT from CICC to DICT

identifies cybersecurity as a high-yield and high-value industry that need to be developed.

- ➡ Outcome 2: Creativity and innovation in services value proposition strengthened.
  - ‣ Ensure the sustainable supply of a competitive, creative, and skilled workforce strategy mentions the need to strengthen collaboration between private and public sector in mentoring programs and in initiatives that aim to develop cybersecurity literacy, among others

- ◉ Chapter 10: Promote competition and improve regulatory efficiency.
  - ➡ Cross cutting strategies: Promote competition and improve regulatory efficiency in and through the internet and digital technologies
    - ‣ Expand access to broadband internet and digital technologies to enhance consumer choice and facilitate digitalization and innovation among micro, small, and medium enterprises strategy mentions the importance of cybersecurity in developing the national broadband plan.
- ◉ Chapter 13: Ensure peace and security and enhance the administration of justice.
  - ➡ Outcome 3: Protection and safety from natural hazards and other security threats
    - ‣ Protect critical infrastructure, strategic assets and natural resources strategy defines critical infrastructure to include information infrastructure.
    - ‣ Strengthen security and resilience of the Philippines cyberspace strategy broadly defines key objectives, all of which are in the NCSP 2023-2028.

Cybersecurity and cyberspace defined

The definition of cybersecurity in the NCSP 2023-2028 (see "Definition of Terms" section in page xi) is in accordance with current Philippine statutes and is aligned to the definitions from the ISO and the United Nations [1] [6]. The adopted definition is also universally accepted [7].

It is no longer sufficient to view cybersecurity strictly within the confines of the CIA triad[2] namely, Confidentiality, Integrity, and Availability. The NCSP 2023-2028 adopts an expanded definition of Cybersecurity using the acronym CIANA-PS[3]. Non-repudiation and authenticity comprise a generally accepted expansion of the usual CIA triad and are explicitly enumerated by both the ISO and ITU as important properties of cybersecurity. Privacy is additionally considered an integral component in cybersecurity [8].

Cyberspace is not bound by physical nor geographical boundaries. To adapt to the vastness of cyberspace, the scope of the NCSP 2023-2028 extends to every asset in cyberspace accessible within the country, regardless of their source or location. The NCSP 2023-2028 does not distinguish whether the information asset resides within or outside the Philippine territory. Consistent with its rights as a nation, the Philippines may act to limit or prohibit access to and from malicious actors and assets in cyberspace to residents of the country, subject to existing laws, rules, and regulations.

[2] CIA = Confidentiality, Integrity, Availability

[3] Please refer to the table of acronyms in page ix

The current Philippine cybersecurity landscape

The Philippines is vulnerable to attacks. Kasperksy reported an increase of 432.75% in web threat attempts to Philippine-based websites from 2021 to 2022 [9].

The Philippine NCERT monitored 57,400 cybersecurity threats, and handled 3,470 incidents from 2021 to February 28, 2023. The top three cybersecurity incidents were: (1) malware / malicious code at 48.9%, (2) Data Leakage (12.5%), and (3) Compromised Websites (12.4%) (Figure 1). An overwhelming majority of these incidents targeted government emergency response systems (61%), the academe (13%), and the telecommunications sector (8%) (Figure 2).

Since the publication of the first NCSP 2017-2022, the country's cybersecurity posture is improving, but not at par with our regional counterparts. From 2017 to 2020, the Philippines improved its Global Cybersecurity Index (GCI) score from 59.4 to 77, but fell in its ranking from 37th out of 193 countries in 2017 to 61st out of 194 countries in 2020[4]. In the ASEAN region, the country was ranked 4th in 2017, but fell to 6th in 2020, behind Vietnam and Indonesia in the latest GCI rankings.

Various laws from other countries also impact the country's cybersecurity landscape. This is especially because the Philippines is one of the top Business Process Outsourcing (BPO) destinations in the world. Among these laws and regulations is the European Union's (EU) General Data Protection Regulation (GDPR) that mandates the adoption of similar standards when processing EU citizen PII. Although the Philippines Data Privacy Act of 2012 was enacted and is at par with international regulations. The EU also enacted the Cybersecurity Act in 2019, imposing security certification requirements not only to EU companies, but also to those that are part of the ICT supply chain for EU companies. Some of these submarine cables of the Philippines end at the United States of America, subjecting its build-out and maintenance to US regulations and permits.

The PDP underscores the importance of cybersecurity in ensuring public trust in e-Commerce and online banking and trade. The Philippine Statistics Authority (PSA)

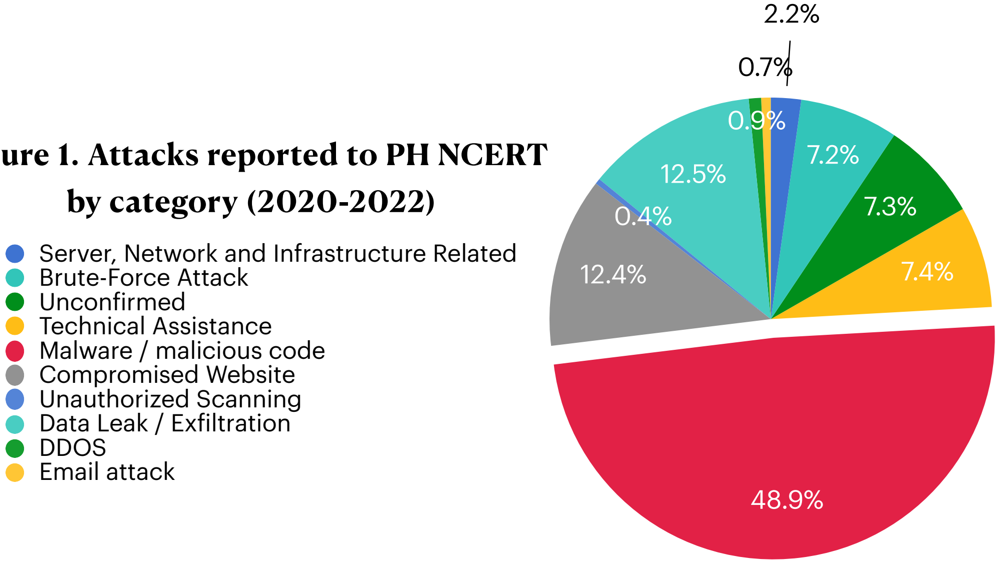


Figure 1. Attacks reported to PH NCERT by category (2020-2022)

[4] https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

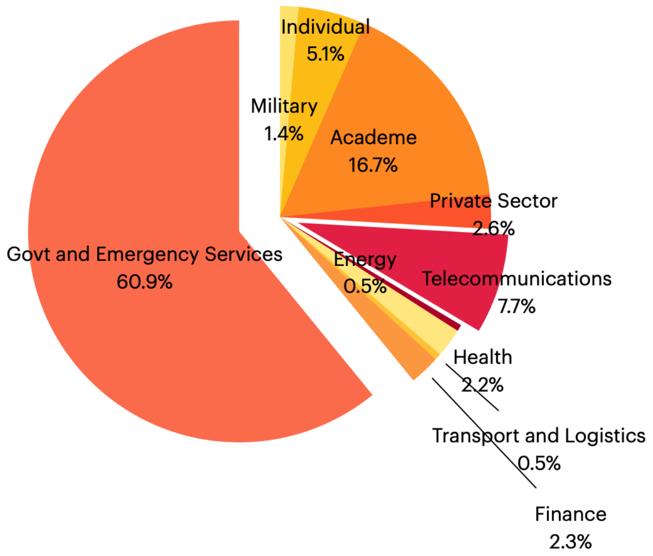
reported a 7.8% increase in the digital economy, from Php 1.73 trillion (~US $32.04 Bn) recorded in 2020 to Php 1.87 trillion (approximately US $34.63Bn[5]) in 2021, which was equivalent to 9.6% of the country's GDP [10]. From this figure, the share of digital-enabling infrastructure (Telecommunications, Professional and Business services, etc.) was 76.9%, and e-Commerce was at 17.6% or approximately Php 329.12 Bn (~US $6.09Bn).

The figures reported by PSA were lower than those forecasted by the Department of Trade and Industry (DTI), as shown in Figure 3 [11]. Interestingly, the DTI forecast also mentioned that, with proper planning such as the development of an e-Commerce roadmap with cybersecurity and building trust at its core, e-Commerce can grow by 3% more by 2025 and 3x more by 2030.

The Information Technology Business Process Management (IT-BPM) industry of the Philippines contributed approximately US $31Bn to US $33Bn revenues in 2022 and employed about 1.5 million Filipinos. The industry is expected to grow with revenues of US $48.5Bn and employ 2.1 million Filipinos by 2028 [12]. IT-BPM is heavily reliant on resilient and secure telecommunications facilities because most of the industry sector clients are abroad, 85% of which are in North America and Europe. The sector also anticipates a sustained move to new workplace environments, such as work-from-home arrangements, thereby increasing the demand for secure and reliable internet connectivity including in residential areas. The security of the subsea cables and the robustness of the telecommunications sector are key drivers of growth for the BPO industry. Cybersecurity plays a tangible and direct role in this area.

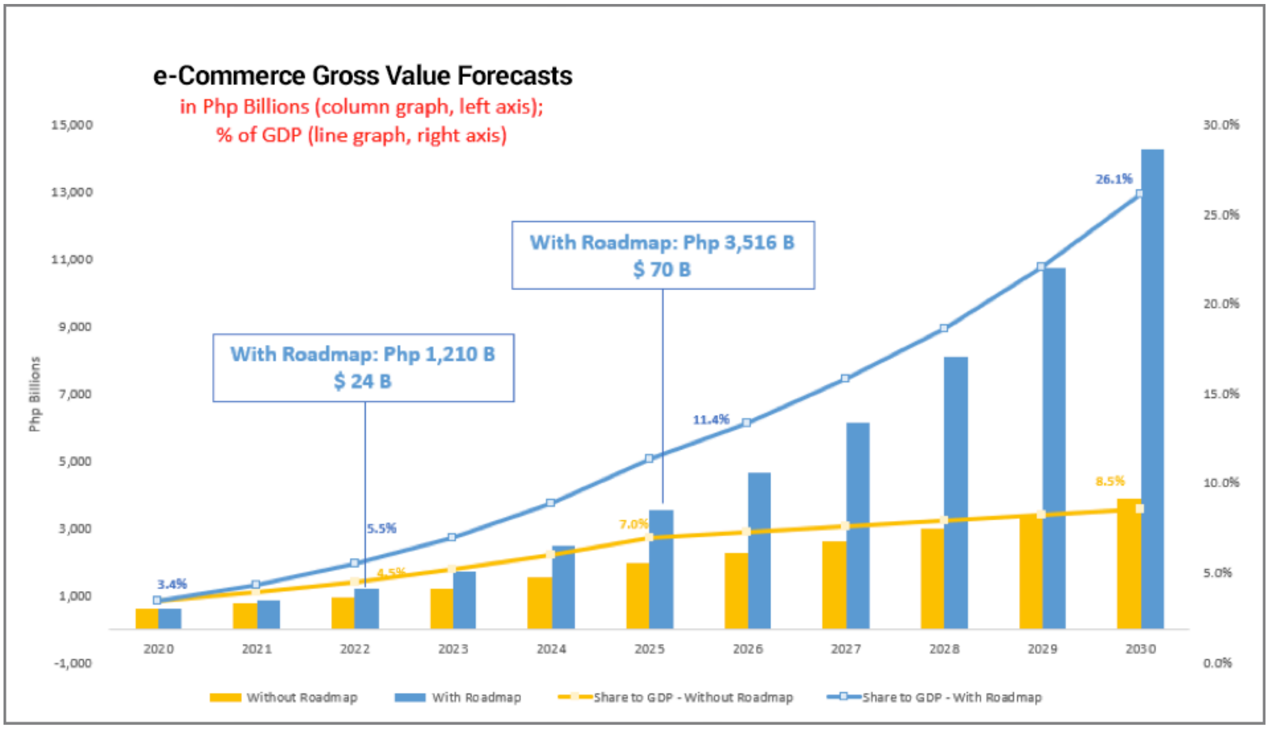
Against this backdrop, the public and private sectors' adoption of cybersecurity policies is poor. Except for exceptionally large enterprises, both government agencies and the private sector are reluctant in investing in cybersecurity. In 2017, the Philippines only

Figure 2. Cybersecurity incidents by target (2022)



[5] At an exchange rate of Php 54 to US $1

Figure 3. e-Commerce Gross Value forecast with and without a Roadmap (source: DTI)



spent 0.04% of its GDP in cybersecurity, while the ASEAN average spending was 0.07% of its GDP [13]. A study of the economics of cybersecurity revealed that policies usually fail when there is: (1) misalignment of incentive between the cost of following the policy versus the cost of not following it; (2) information asymmetries that promote one-sided economic relationship in favor of the producer thus encouraging 'lemons'; and, (3) externalities [14]. Discussion of these factors is beyond the scope of the NCSP 2023-2028. An elaboration on the economics of cybersecurity and how these three factors affect policy adoption can be found in the citations [15].

Vision: *trusted, secure, reliable cyberspace for every Filipino*

The vision enumerates three collectively desired goals for securing the nation's cyberspace.

TRUSTED. The most important factor in e-Commerce, digital trading, and online banking is trust. Institutionalizing trust by strengthening the country's capability to secure transactions in cyberspace, as defined in the PDP, is undeniably important to the country's economic growth. Improving trust requires reducing the social and technical opaqueness and complexity [16] of the internet. Trust involves at least two parties and usually signifies a positive expectation that the action of the other party will take into account the best interest of both parties [17]. It involves the firm belief that a trustee will not perform an action detrimental to the trustor, regardless of the ability of the latter to monitor and control the trustee [18]. This confidence translates to reduced worries on risks occurring, even when the system provider is not transparent on how the IS is built and maintained.

A *network of trust* among different parties, namely, the user, the information system, the information system provider, and other other vendors in the ICT system supply chain, is required in cyberspace [19]. Key to earning this trust is the provision of sufficient information among parties. A trustor should have enough knowledge to make an informed decision on whether to trust or not to trust an IS in cyberspace. These are attained by providing accurate and complete information about all actors involved in the building, maintenance, and the use of an IS. This is where supply chain security of ICT becomes critical. For the public, an easy-to-understand certification system based on facts is equally important.

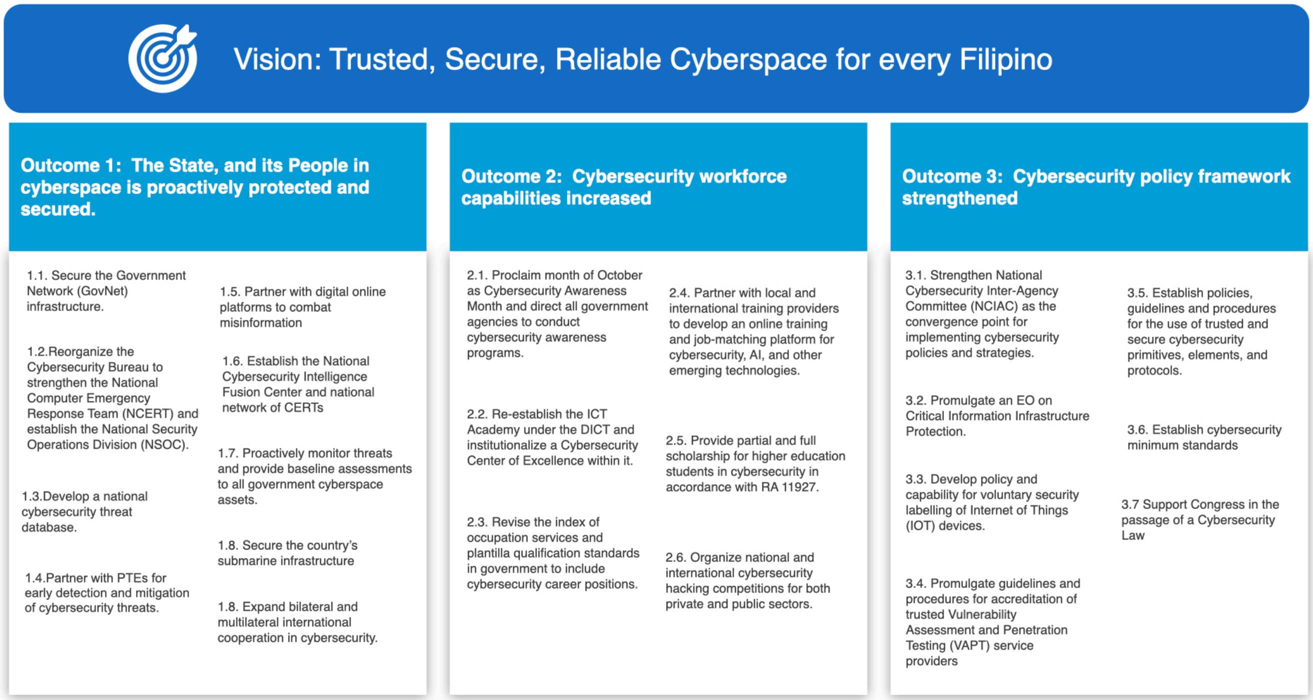
SECURE. Security refers to the protection of assets in cyberspace. Assets include intangible and tangible assets. Admittedly, not all assets can be fully protected from an evolving landscape of threats, vulnerabilities, and threat actors. The adoption of a risk-based approach is required to effectively secure information assets in the cyberspace.

RELIABLE. Reliability refers to the consistency of a system in performing its intended behavior or achieving results [1]. While assets should be protected from intentional failures, unintentional or accidental failures should also be properly mitigated through redundancy of systems and processes. A system is regarded as unreliable based on the frequency of observed failures. Reliability also affects the quality of service because non-reliable systems will not be able to ensure the continued achievement of service expectations. Thus, by including reliability in the vision, it becomes the nation's goal to develop an ecosystem of quality ICT products that deliver services as advertised. There should be a mechanism to be established to monitor and ensure reliability of the country's ICT products.

The NCSP 2023-2028 results framework

Figure 4 shows the framework of the NCSP 2023-2028. To realize the vision, three desired outcomes are aimed to be produced as a result of the implementation of identified strategies.

Figure 4. NCSP 2023-2028 Results Framework



Vision: Trusted, Secure, Reliable Cyberspace for every Filipino

Outcome 1: The State, and its People in cyberspace is proactively protected and secured.

1.1. Secure the Government Network (GovNet) infrastructure.

1.2.Reorganize the Cybersecurity Bureau to strengthen the National Computer Emergency Response Team (NCERT) and establish the National Security Operations Division (NSOC).

1.3.Develop a national cybersecurity threat database.

1.4.Partner with PTEs for early detection and mitigation of cybersecurity threats.

1.5. Partner with digital online platforms to combat misinformation

1.6. Establish the National Cybersecurity Intelligence Fusion Center and national network of CERTs

1.7. Proactively monitor threats and provide baseline assessments to all government cyberspace assets.

1.8. Secure the country's submarine infrastructure

1.8. Expand bilateral and multilateral international cooperation in cybersecurity.

Outcome 2: Cybersecurity workforce capabilities increased

2.1. Proclaim month of October as Cybersecurity Awareness Month and direct all government agencies to conduct cybersecurity awareness programs.

2.2. Re-establish the ICT Academy under the DICT and institutionalize a Cybersecurity Center of Excellence within it.

2.3. Revise the index of occupation services and plantilla qualification standards in government to include cybersecurity career positions.

2.4. Partner with local and international training providers to develop an online training and job-matching platform for cybersecurity, AI, and other emerging technologies.

2.5. Provide partial and full scholarship for higher education students in cybersecurity in accordance with RA 11927.

2.6. Organize national and international cybersecurity hacking competitions for both private and public sectors.

Outcome 3: Cybersecurity policy framework strengthened

3.1. Strengthen National Cybersecurity Inter-Agency Committee (NCIAC) as the convergence point for implementing cybersecurity policies and strategies.

3.2. Promulgate an EO on Critical Information Infrastructure Protection.

3.3. Develop policy and capability for voluntary security labelling of Internet of Things (IOT) devices.

3.4. Promulgate guidelines and procedures for accreditation of trusted Vulnerability Assessment and Penetration Testing (VAPT) service providers

3.5. Establish policies, guidelines and procedures for the use of trusted and secure cybersecurity primitives, elements, and protocols.

3.6. Establish cybersecurity minimum standards

3.7 Support Congress in the passage of a Cybersecurity Law

Outcome 1: The state, and its people in cyberspace is proactively protected and secured

Cyberspace has been weaponized to deliver two broad types of operations: (1) As preparation for kinetic warfare and (2) information operations to destabilize governments through subversion and coercion [20].

Many countries view cybersecurity as the fifth domain in national defense and security [21]. Other countries, however, that are yet to announce the same military doctrine, are also often seen exploiting cyberspace. In December 2015, Ukraine's power grid was hacked causing loss of power for 30 substations located in the Ivano-Frankivsk region, consequently affecting 23,000 residents. This successful cyberattack of a power grid is a clear demonstration of how operations in cyberspace can support traditional kinetic wars by taking down civilian critical infrastructures.

The second type of cyberattack is information operation, or sometimes referred to as cognitive warfare. It is defined as the actions taken by state or non-state actors to distort domestic or public political sentiments usually through the use of social media [22].

To mitigate these threats, the country must secure and protect CII. The national broadband and government data centers must also be secured and protected. To ensure efficient response and resolution of cybersecurity incidents, a network of CERTs must be established between CIIs which are usually private enterprises and government agencies, including LGUs. A national framework for incident response should also be cascaded to facilitate faster and easier communication among different CERTs locally and internationally. Establishing working relationships with social media platforms and promoting industry self-regulation regarding disinformation and fake news are also strategies under this outcome.

Another important factor that significantly affects Outcome 1 is the proper implementation of other complementary national strategies developed by other government agencies on cybersecurity. These include the National Security Strategy, National Defense Plan / Strategy, and the National Cybercrime Strategy. These strategies work seamlessly with the NCSP 2023-2028 and as a whole contributes to the success of Outcome 1.

1.1. Secure the Government Network (GovNet) infrastructure

The GovNet project is part of the National Broadband Program (NBP) of the DICT. The project aims to interconnect more than 3,900 national and local government agencies and units to the 5,414 km National Fiber Backbone (NFB) of the NBP. As of December 2023, GovNet is 30% complete. But most of these still go through the PTEs.

The GovNet project shall be re-calibrated to ensure it is secure-by-design. A comprehensive cybersecurity defense system for GovNet shall be developed by DICT, along with DOST and NTC. Apart from strategically positioning IDS, IPS, SOAR and SIEMs, GovNet should include protective passive network elements and secure BGP routing into the design. The goal is for all government agencies to operate under a secure unified Wide Area Network (WAN).

The DICT National Government Data Center (NGDC) project shall also be recalibrated. The goal is to build a secure national government cloud platform to store highly classified government data. These data centers should follow international standards in information security and should be secure by design. Other government data can still be stored in commercial public clouds, provided that there are appropriate technological and legal controls to ensure confidentiality, integrity, and availability of the data. A good standard to follow when securing data stored in the public cloud is [23].

DICT shall coordinate with the DND, AFP, and PNP to secure the physical internetwork of GovNet and the NFB, including the landing stations and submarine cable systems that it connects to.

1.2. Reorganize the Cybersecurity Bureau to strengthen the National Computer Emergency Response Team (NCERT) and establish the National Security Operations Center

The DICT currently operates the National Computer Emergency Response Team (NCERT) and a National Security Operations Center (NSOC) under its Cybersecurity Bureau (CSB). With less than 30 people, the current NCERT handles cybersecurity incident response, cybersecurity incident investigation, government VAPT services, threat monitoring, threat hunting, malware analysis, threat advisories, and training on incident response, among others.

The plan is to expand NCERT to allow it to operate nationwide with the capability to respond on-premise should a major cybersecurity incident is reported. The NCERT shall also be divided into two divisions: (a) the Computer Emergency Response Team which shall focus only on cybersecurity incident response and investigation; and, (b) the National Security Operations Center (NSOC) division whose main responsibility is to monitor critical information assets in cyberspace, perform VAPT services, and conduct baseline assessment of government agencies' cybersecurity posture.

The two divisions shall be under DICT-CSB and shall operate twenty-four hours a day, seven days a week (24x7).

The current physical National Security Operations Center shall also be modernized to allow it to monitor cybersecurity of government agencies. This includes a centralized incident response system for government that allows NSOC to delegate incident tickets to other civilian government agencies and units and to monitor their progress. Cybersecurity teams within each government agencies and units shall have access to the same cybersecurity incident response ticketing system, ensuring a single view of all cybersecurity incidents.

Private sector organizations and enterprises classified as CII shall be required to form their own cybersecurity teams and shall coordinate regularly with the NSOC division of the DICT-CSB.

1.3. Develop a national cybersecurity threat database

The DICT shall develop a national cybersecurity threat database which shall be accessible to the public. The list of threats should be curated based on the category of the threat and the type of the threat (e.g. TTP, vulnerability class, malware type, etc.) based on their CVSS score, category and type. The threat database shall be updated regularly. Both the public and private sectors can download threat data and feeds from this database in a common format, such as in CSV, to easily reformat and upload the data to any cybersecurity defense systems such as, but not limited to, firewalls, web application security systems, and protective DNS, etc.

The DICT shall also develop and maintain a website to inform the public of the latest trends in cybersecurity and to issue advisories.

1.4. Partner with PTEs for early detection and mitigation of cybersecurity threats

A meaningful partnership with PTEs is important in securing cyberspace. The NCERT gets reports both local, and international, on attacks emanating from within our local PTE networks which need to be acted on. These malicious computers are usually behind CGNATs and thus can only be identified by the PTEs. PTEs also operate most of the Cable Landing stations which need to be secured.

1.4.1. Agree on minimum requirements for management of CPE and network segments for ISPs and Telcos

Data from our NCERT shows that malware is a top security threat. The Mirai malware outbreak in 2014 illustrated how IOT devices can be compromised at a massive scale. There is a global consensus that this trend will continue in the near term [24]. Various studies showed that PTEs and ISPs are critical control points in the fight against malware and botnets [25], since approximately 87% of the compromised devices reside within access points or within customer premises of ISPs [24]. To mitigate the threat of malware and botnets in the country, the DICT, NTC, and all PTEs and ISPs should agree on protocols for reporting botnets and hacking activities emanating from within PTE and ISP networks. These include assisting in investigations of the DICT, CICC, PNP, NBI and other government agencies regarding botnet attacks, illegal access to computers, DDOS attacks, etc.

PTEs and ISPs have several countermeasures that are proven effective against malware [26]. Research also showed that ISPs will gain economically from mandatory notification and voluntary cleanup of their networks [27]. The following countermeasures can be studied:

1. Security-harden their Customer Premise Equipment (CPE) such as changing the default password and disabling unused TCP/IP protocol ports;
2. Provide assistance by allowing government to use the telco and ISP email and messaging systems for cybersecurity campaigns;
3. Provide for a voluntary malware cleanup facility for their customers;
4. Comply with government requests for identifying and managing network elements that are mounting a DDOS attack or reported to be part of a command and control structure of a ransomware, malware, or botnet; and,
5. Implement technological controls to mitigate the threat of SMS scam, spam, and phishing.

To assist ISPs and telcos, the government shall invest in network elements that are common among ISPs and that can be issued by telcos as anchors of trust. The government can also provide a webpage containing instructions for malware clean-up using free anti-malware software and diagnostic tools.

1.4.2. Define and implement standards to protect inter-domain IP routing protocols

The NTC shall lead in forming a multi-sectoral Technical Working Group (TWG) with the DICT and DOST to propose standards for securing inter-domain routing protocol, especially Border Gateway Protocol (BGP). *The goal is to attain national compliance for securing inter-domain routing for all AS located in the Philippines, including telco-to-customer AS by 2026*.

BGP is the de facto routing protocol of the internet and is considered an un-secure routing protocol despite its critical role in the internet. In BGP, any Autonomous System (AS) can advertise a prefix for an unassigned IP address space belonging to another AS. Neighboring AS receiving this announcement may also advertise the wrong prefix, thus directing a route to a wrong AS. This is called prefix hijacking. Prefix hijacking is commonly due to misconfigurations, although a malicious AS or sub-AS can use this technique as a form of attack [28].

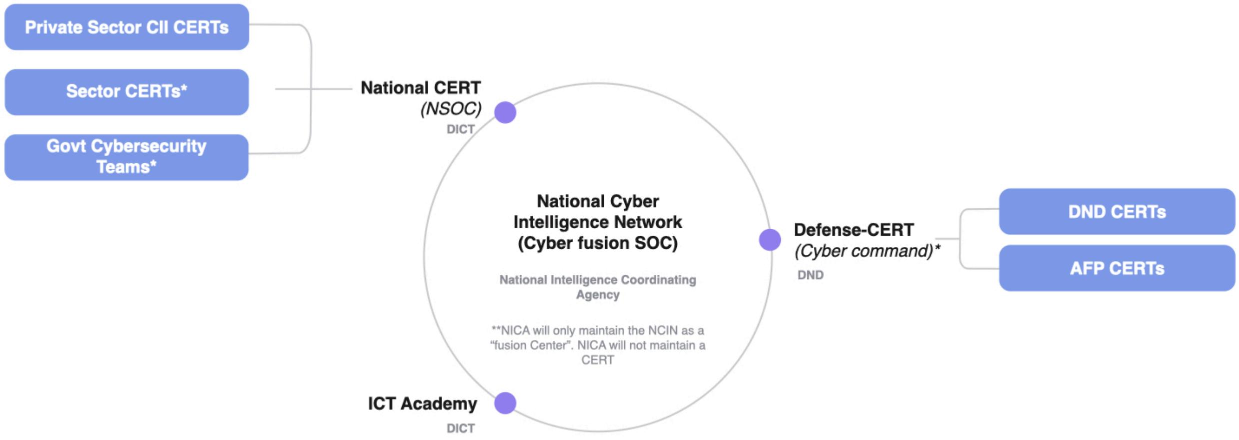
Spammers, phishing sites, and scammers are also known to deliberately inject incorrect BGP information to hide their tracks when using e-mail servers or when impersonating websites. Indeed BGP remains vulnerable to attacks and misconfigurations that may cause disruption in the global internet routing system, damage to cryptocurrencies, anonymization of networks, and cloaking of cybercriminal activity [29].

There are various ways to secure BGP, which are contained in several Internet Engineering Task Force (IETF) standards. Among the most prominent recommendations of IETF is the use of Secure-BGP or S-BGP [30]. There is, however, poor adoption of S-BGP due to computational latency, increased bandwidth, and storage overhead [29]. The US NIST proposal on Route Origin Validation (ROV) may be considered as an alternative [31] [32].

1.5. Partner with digital online platforms to combat misinformation

The DICT shall forge a deep and meaningful partnership with digital online and social media platforms to create a mutually acceptable protocol for reporting, correcting and mitigating misinformation, and online harms. The agreement to be forged shall be in line with the UNESCO report that acknowledged the need to regulate digital online platforms, including social media platforms, where people sow disinformation that may affect public trust, national issues, and promote terrorist activities and self-harm [33]. The objective is for DICT, through the NCERT, to promptly report concerns or issues to the management of digital online and social media platforms for immediate resolution. The partnership with digital online platforms will ease the process of reporting by the government and facilitate the resolution of hacking incidents of government social media accounts.

Figure 5. The nationwide CERT and SOC model


Private Sector CII CERTs
Sector CERTs*
Govt Cybersecurity Teams*
National CERT
(NSOC)
DICT
National Cyber Intelligence Network (Cyber fusion SOC)
National Intelligence Coordinating Agency
**NICA will only maintain the NCIN as a "fusion Center". NICA will not maintain a CERT
Defense-CERT
(Cyber command)*
DND
DND CERTs
AFP CERTs
ICT Academy
DICT

1.6. Establish the National Cybersecurity Intelligence Fusion Center and national network of CERTs

The strategy is to rationalize the network of CERT nationwide, define delineation of duties to avoid overlap of functions, and to clearly define the coordination and hierarchy of CERTs that shall act during computer emergencies. All CERTs must work within a strict chain of command with the two top-level CERT, namely, the DICT NCERT and the Defense-CERT, coordinating each other's efforts. The National Cybersecurity Intelligence Network (NCIN) shall act as a cyber fusion center providing important situational awareness to both the civilian CERTs through the NCERT, and the Defense-CERT. There shall also be a national framework for responding to cyber incidents to ensure unity in triaging, classifying, and managing cybersecurity incidents.

Personnel of the NCERT and the Defense-CERT shall have the proper clearances to access confidential information.

1.6.1. Clearly defined roles of the different CERTs

Figure 5 shows the 2-CERT/3-SOC model at the national level. In the Philippines, a Computer Security Incident Response Team (CSIRT) is also called as a Computer Emergency Response Team or CERT. Under RA 10844, the DICT maintains the National CERT (NCERT), which is officially registered in the international community as CERT-PH. For consistency, the NCSP 2023-2028 refers to CERT-PH only as NCERT.

Generally, a CERT is an organization that provides services and support to detect, prevent, and respond to cybersecurity incidents [34] [35].

There are many categories of CERTs based on their scope or constituencies [36]. Using the same criteria, the NCSP 2023-2028 identifies three types of CERT that interoperate.

1. ***Organization CERT*** - The most basic type of CERT. An organization CERT responds to cybersecurity incidents within an organization. An example of an organization CERT are CERTs operating within the CII, LGUs, schools, and NGAs, among others. The organization CERT is tasked to respond to cybersecurity incidents, regardless of their

complexity or criticality, while other coordinating CERTs such as the NCERT or SCERT will only provide specialist support and information to the organization CERT.

2. ***National coordinating CERT*** - Their main function is to coordinate information sharing and response through the various organization CERTs. Coordinating CERTs do not normally respond directly to a detected cybersecurity incident, but instead calls on the organization CERT to deal with the incident. Coordinating CERTs conduct training and exercises to various CERTs and define the framework and procedures to resolve cybersecurity incidents.

3. ***Sector coordinating CERT (SCERT)*** - The SCERT is also a coordinating CERT. An SCERT is created for regulatory agencies that regulate important sectors with various CII CERTs. The formation of an SCERT is optional. An SCERT exists because of recognized peculiarities and unique situations where a CII operates on. For example, the banking industry operates under strict regulations, including necessity of keeping accounts secret; hence, reporting of a cybersecurity incident of a bank may be coursed first to its regulator, the BSP, that operates as an SCERT. The NCSP 2023-2028 directs that a CII shall report a critical or severe cybersecurity incident to both the NCERT and the SCERT, but it will be the SCERT that will directly assist the organization CERT.

A Security Operations Center (SOC) is a facility that monitors systems and networks for malicious behavior and for indications of a potential cyber-attack. The SOC provides situational awareness for the CERT and serves as a proactive mechanism to detect, analyze, and respond to cyberthreats. While a CERT refers to the organization that responds to cybersecurity incidents as mandated to handle cybersecurity incidents, a SOC is the set of tools and people monitoring cyberspace and determining genuine cybersecurity incidents that should be responded to [36].

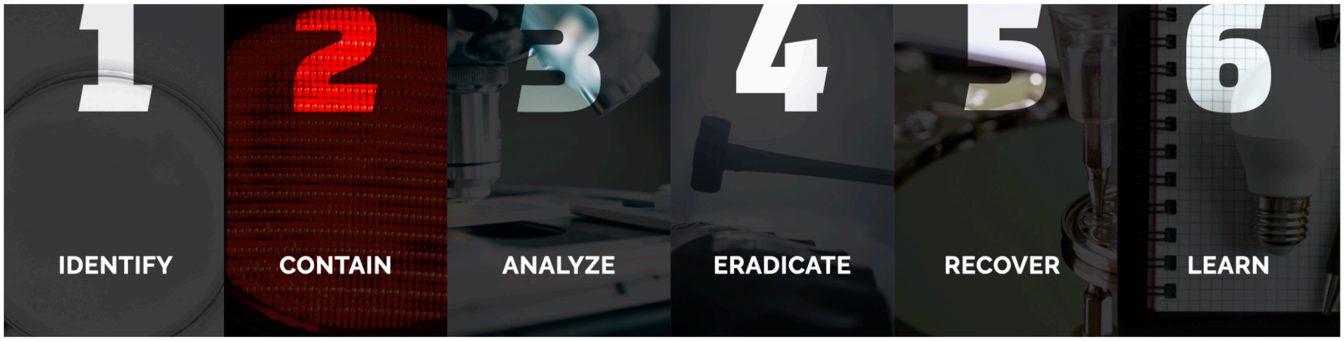
Like CERT, there are many types of SOC. One important type of SOC is called a "cyber intelligence fusion center" which is a SOC that primarily aggregates and analyzes information between two or more SOC [34]. The NICA shall develop the National Cyber-Intelligence Network or NCIN which is the Philippine version of a cyber intelligence fusion center type of SOC.

There shall be two national coordinating CERTs: (1) NCERT managed by the DICT and whose primary function is to act as the coordinating CERT for all government and CII organization CERT as per RA 10844 and (2) Defense-CERT which is the national coordinating CERT for AFP-CERTs and state-sponsored cybersecurity incidents.

There shall be three SOCs: (1) the NCIN, which is the cyber-intelligence fusion SOC, (2) the NSOC managed by the NCERT, and (3) a Cyber Command, a SOC within the AFP but under the Defense-CERT. The NCIN's main objective is to provide overall situational awareness in cyberspace. Thus, it will receive data directly from the NSOC and the Cyber Command. Once NCIN determines that a series of cybersecurity incidents are attributable to a state-sponsored threat actor, NCIN shall inform NCERT, and NCERT shall handover the response activities to the Defense-CERT. The DICT and DND, together with the NSC and NICA, shall develop the handover and communications procedures between the two national coordinating CERTs and the three national SOCs.

2.2.2. Adoption and Implementation of the six-stage Cybersecurity Incident Response Model

Figure 6. Cybersecurity Incident Response Model



Shown in Figure 6 is the adopted National Cybersecurity Incident Response Model. The model is similar to most cybersecurity incident response models from other countries and has a resemblance to the NIST cybersecurity framework [37]. This model is essential in ensuring uniformity of actions of private and government organizations when addressing cybersecurity incidents. This also eases coordination of the NCERT and SCERT to all organization CERTs and facilitates faster and more efficient communication between parties during emergency situations.

1. ***Identify*** - The focus during this phase is to describe the incident by answering the 5Ws and 1H (what, when, who, where, why and how). The question "why" the cybersecurity incident happened may not yet be known. At this stage, the organization CERT shall assign a criticality level to the incident. The issue resolution shall also be assigned to an incident response agent or team.
2. ***Contain*** - To contain means to mitigate the potential spread of the incident to other assets, such as if it is a ransomware or malware, initial steps must be taken to ensure that the malware does not spread by isolating the infected machines or quarantining identified infected files. The response at this stage varies by type of cybersecurity incident.
3. ***Analyze*** - This stage focuses on finding the root cause. Normally, a CERT will proceed to analyze only after the incident is sufficiently contained, although a large CERT with dedicated teams may simultaneously conduct containment and analysis. At the latter case, the CERT should be careful to ensure that the "analysts" do not hamper the activities designed to contain the incident.
4. ***Eradicate*** - At this stage, the identified root cause of the issue is removed or remediated. This stage is not purely technical. Some root causes can be eradicated by changes in procedure, such as a successful spear phishing attack against the head of a government agency which can be addressed by changing the account credentials of the user and removing email addresses of senior officials at public websites.
5. ***Recover*** - The focus of the activities at this stage is to revert the affected information asset back to its normal operating parameters. For example, a data backup may be used to revert data to an acceptable recovery time objective. Recovery may also refer to reverting the organization back to its normal state. After a successful recovery and the cybersecurity incident is declared closed, the next stage occurs.
6. ***Lessons Learned*** - the final stage of the six-stage cybersecurity incident response model is where documentation is done to record lessons learned and to review and consider adoption of procedures and controls implemented for future incidents. During

this stage, the CERT may also identify processes and steps that should be improved or require correction. Good practices are also documented. The organization CERT shall complete their detailed report for submission to the SCERT and the NCERT.

DICT shall revise and update its manual of operation to reflect the new national cybersecurity incident response framework. The manual of operation shall also include (1) vulnerability scoring mechanisms; (2) information sharing mechanisms including traffic light protocols; (3) response times based on severity, and reporting hierarchy.

1.7. Proactively monitor threats and provide baseline assessments to all government cyberspace assets

The DICT, with the assistance of the DOST, shall develop the capability to automatically scan all government and critical information infrastructure assets exposed in the internet for their vulnerabilities, and provide a risk score to these scanned threats. The scores and vulnerability scanned shall be kept confidentially and shall be provided to the owners of the scanned cybersecurity assets. Owners of these compromised assets should report to DICT how they mitigated the vulnerabilities. DICT should check if the vulnerabilities were indeed resolved.

The DICT shall develop and/or acquire the necessary tools to ensure that the assessments are stored and disseminated to all government agencies.

Private security research should be allowed to report their findings in a safe environment, free from litigation. The DICT shall issue the necessary guidelines for responsible disclosure of government vulnerabilities.

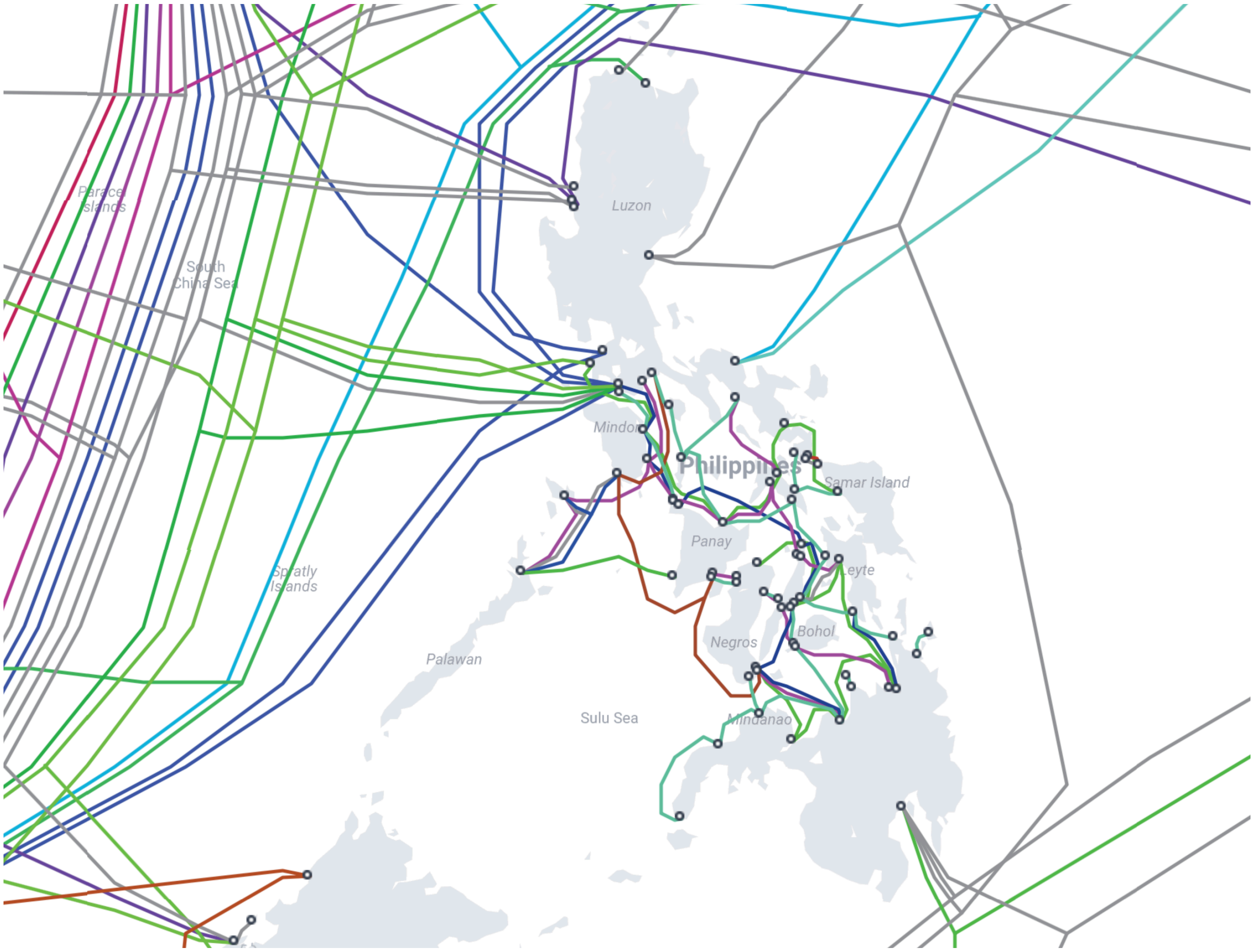
A monthly report of these baseline scores shall be submitted to the Chairpersons of the NCIAC and to the Office of the President.

1.8. Secure the country's submarine cable infrastructure

As of this writing, there are 11 international cable landing stations in the country and at least six more inter-Asia and trans-pacific submarine cables planned to land in the Philippines. More than half of these submarine cables go through contested waters, either in the West Philippine Sea and the Taiwan Strait. There is also a significant network of submarine cables operated by PTEs some in consortium with international submarine cable operators.

These submarine cables are often damaged due to pilferage, anchorage, earthquakes, and major climate disturbances, to name a few. The average time to repair submarine cables in the West Philippine Sea is 130 days above the global average [38] due to competing requirements for licenses to operate submarine cables and lack of submarine cable repair vessels in the area. This poses a threat to the BPO industry which is one of the major drivers of the Philippine economy. To mitigate these threats, the DICT needs to seek the assistance of other government agencies such as the Philippine Coast Guard (PCG) in securing submarine cables and cable landing stations. DICT should also coordinate with other government agencies and private consortiums to develop a map of all submarine cables laid out throughout the country.

Figure 7. Submarine Cable Map of the Philippines



1.9. Expand bilateral and multilateral international cooperation in cybersecurity

The country shall pursue confidence-building measures to avoid conflicts in cyberspace. This can be done by expanding existing agreements with InterPol, UN, and the ASEAN, as well as its bilateral agreements with our allies for cybersecurity capacity building, information sharing, and technical assistance.

In the ASEAN, the country shall proactively increase its participation in various bodies where cybersecurity issues are discussed including: (1) the ASEAN Foreign Ministers' Meeting (AMM); (2) the ASEAN Digital Ministers Meeting (ADGMIN); (3) the ASEAN Regional Forum (ARF) which focuses on confidence-building measures among members; (4) the ASEAN Defense Ministers' Meeting-Plus (ADMM-Plus) which focuses on cybersecurity issues related to defense and military sectors; and (5) the ASEAN Ministerial Meeting on Transnational Crime (AMMTC) which focuses on cybercrime. The country shall also increase its engagement in the ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC). The body coordinates discussions at the various ASEAN bodies.

The country agrees with the Eleven Norms of Responsible State Behavior by the UN Open-Ended Working Group (OEWG) and is supportive of its adoption by the UN General

Assembly. These norms have been the product of the UN Group of Governmental Experts (UN GGE)[6] from 2004 to 2021. Substantive discussions are continuing, and the Philippines is hopeful that these norms will continue to be developed. At the regional level, the country shall support the establishment of mechanisms and confidence-building measures leading towards a safe and responsible behavior of all states in cyberspace.

In general, the country's presence is required in the international arena to engage our allies, friends, and counterparts in a discussion for mutual benefit and respect. While there is also a tendency for events in the cyberspace to escalate, it is to the best interest of the country to become active partners in the promotion of responsible and ethical behavior among nations and states in cyberspace and to engage state actors exhibiting irresponsible behavior in the internet through peaceful means.

Outcome 2: Cybersecurity workforce capabilities increased

Globally, recruitment and retention of cybersecurity talent remain as obstacles for most organizations. The World Economic Forum (WEF) reported that only 46% of surveyed cybersecurity leaders in 2022 believed that they have the appropriate personnel with enough skills for their cybersecurity needs. There is a critical skills gap among cybersecurity professionals. This skills gap is higher for the energy, public, and banking and finance sectors [40]. In the Philippines, the IT-Business Process Management Association of the Philippines (IT-BPAP) listed cybersecurity skills at high demand, exacerbated by the shortage of a skilled workforce. Capacitating our workforce and closing the skills gap in cybersecurity is therefore an important strategy in achieving our vision. Thus, under this outcome, six strategies all focusing on cybersecurity awareness of the general population, and ensuring that the country produces the required number of cybersecurity professionals in both the private and public sectors.

Providing equal access to cybersecurity education to the marginalized sectors is a contributor to promoting cybersecurity among the general population. Opening opportunities to majority of the citizens will increase the number of cybersecurity professionals in the country. Thus, equity of access to cybersecurity education is part of the overall cybersecurity workforce strategy.

2.1. Proclaim month of October as Cybersecurity Awareness Month and direct all government agencies to conduct cybersecurity awareness programs

In 2023, the President signed Proclamation Number 353 changing the celebration of the Cybersecurity Month from September to October of every year. This coincides with the de facto international cybersecurity month celebrations. As per the proclamation, all

[6] A good discussion on the development of the norms of responsible state behavior in the GGE, and similar works in international bodies can be found in [39] P. Meyer, "Norms of Responsible State Behaviour in Cyberspace," in *The Ethics of Cybersecurity*, M. Christen, B. Gordijn, and M. Loi Eds. Cham: Springer International Publishing, 2020, pp. 347-360.

government agencies are enjoined to perform cyber-hygiene activities and other awareness campaigns on this month.

2.2. Re-establish the ICT Academy under the DICT and institutionalize a Cybersecurity Center of Excellence

DICT shall re-establish the ICT Academy to foster the development of a highly skilled workforce capable of addressing the challenges posed by evolving cybersecurity landscape. Within the academy, a Cybersecurity Center of Excellence (CCE) will be institutionalized. This center will play a pivotal role in elevating the standards of cybersecurity education and research. It will serve as a focal point for collaborative efforts, bringing together experts, educators, and industry professionals to share knowledge, conduct research, and develop innovative solutions to counter emerging cyber threats.

Moreover, the CCE will actively engage in research initiatives, aiming to contribute to the body of knowledge in cybersecurity. Collaborations with industry partners, government agencies, and international counterparts will be sought to ensure a holistic and globally relevant approach to addressing cybersecurity challenges.

2.3. Revise the index of occupation services and plantilla qualifications standards in government to include cybersecurity career positions

The DICT and DBM shall work together with the CSC to: (1) update the index of occupations by adding ICT and cybersecurity career service positions in government; (2) develop the Qualification Standards (QS) and the Competency Standards (CS) for hiring cybersecurity career service personnel in government; and, (3) create several separate certification pathways for Career Service Eligibility (CSE) for ICT and cybersecurity professionals. For Item 3, the DICT can use Presidential Decree 1408 to create ICT and cybersecurity-centric examination as basis for awarding CSE for cybersecurity positions in government [41]. Apart from PD 1408, the government shall also encourage awarding CSE through internationally recognized cybersecurity certifications whose examination and credentialing system is similar or more advanced than the current CSE examination and credentialing system. This system of equivalency between an industry-recognized certification and career service eligibility is already being done in other countries. For example, the CISSP certification by the ISC2 is considered by the US Department of Defense (DoD) as a DoD-approved 8570 baseline certification with an Information Assurance Technical (IAT) and Information Assurance Manager (IAM) Level 3[7].

DICT and DBM shall also develop a plan to include cybersecurity divisions in each national level government agency. The military shall also create career paths based on their own rules and regulations for cybersecurity positions. The PNP and other uniformed personnel shall also develop career paths for cybersecurity personnel and officers in their own organizations.

[7] The list of DoD approved 8570 baseline certifications for security roles can be found here: https://public.cyber.mil/wid/cwmp/dod-approved-8570-baseline-certifications/

2.4. Partner with local and international training providers to develop an online training and job-matching platform for cybersecurity, AI and other emerging technologies

The DICT shall also develop short courses geared toward up-skilling and re-skilling of the workforce. Internationally recognized certifications in cybersecurity, such as, but not limited to, Certified in Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and Certified Information Security Auditor (CISA), should be encouraged, and the development of a cybersecurity professional organization should be promoted.

These courses will then be made available online. To improve the relevance of these training courses, private industry leaders shall be tapped. These trainings must be well curated and developed to ensure their relevance to job requirements by both the private and public sector.

2.5. Provide partial and full scholarship for higher education students in cybersecurity in accordance with RA 11927

The CHED and the state university and colleges should be encouraged to develop Cybersecurity degree programs. There should also be sufficient pathways for up-skilling and re-skilling existing workforce to allow them to transfer or progress in the cybersecurity profession. DICT should partner with TESDA in developing a National Certification (NC) various cybersecurity skills such as SOC analysts, among others.

In order to encourage more graduates of these formal courses, the Interagency Council for Development and Competitiveness of Philippine Digital Workforce [42] should include Cybersecurity and Information Security studies for partial and full subsidy, subject to the rules and regulations as may be adopted by the council.

2.6. Organize national and international hacking competitions for both private and public sectors

DICT should create linkages with international organizations and governments to develop local cybersecurity talent through their exposure in international competitions. Annually, the DICT shall organize a regional hacking competition which shall culminate in a national hacking competition. The winners of these national hacking competitions shall be sent to select international competitions.

To ensure the continuing development of the competitors and the quality of the competitions, the DICT shall build a network of subject matter experts, resource persons and trainers. DICT shall also provide laboratories such as cyber ranges and compile materials that can be used as resources for training the competitors.

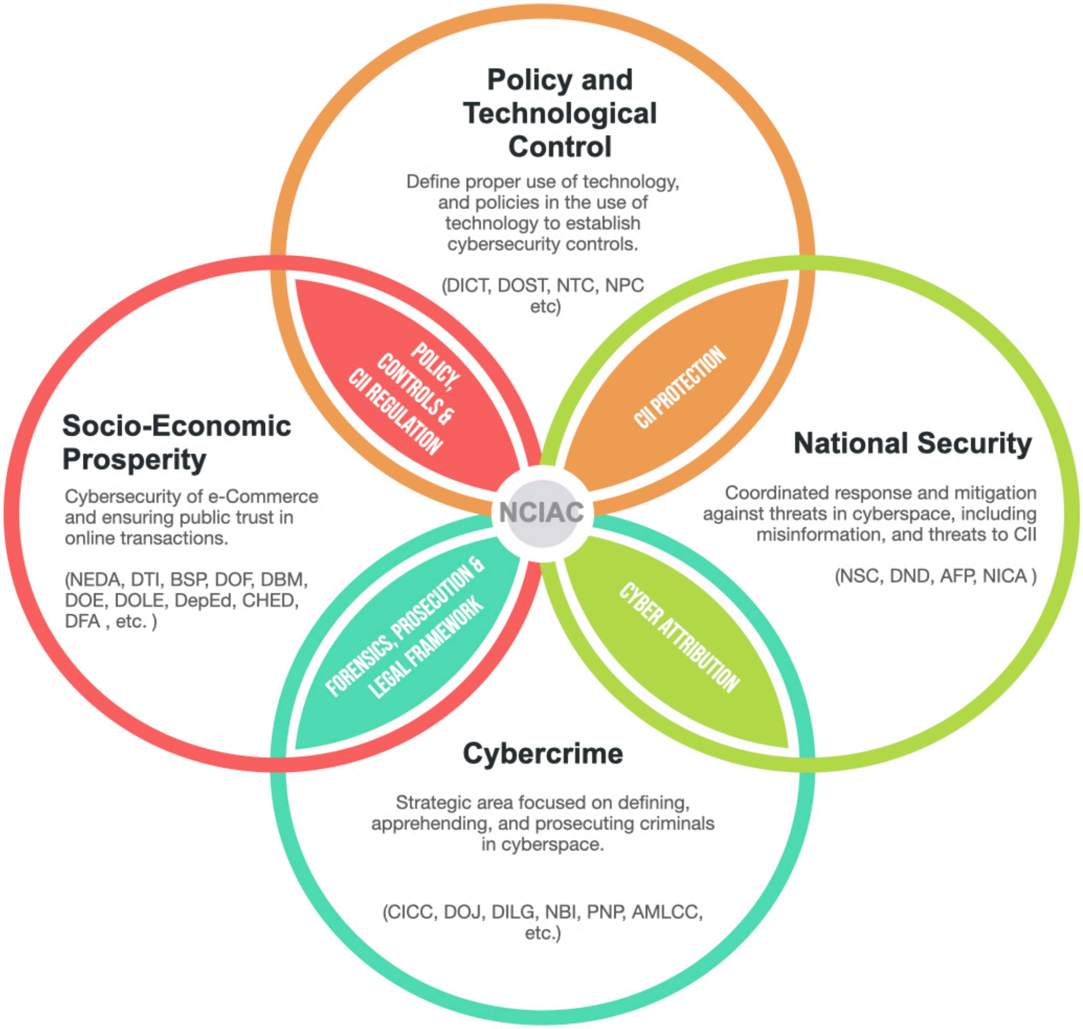
Outcome 3: Cybersecurity policy framework strengthened

The DICT, as the lead agency for cybersecurity policy and implementation, shall ensure that the implementation of existing laws, rules and regulations related to cybercrime and cybersecurity are monitored and enhanced. The DFA shall also engage the international community to ensure our interests in a trusted, secure and reliable cyberspace is protected. New legislative measures shall be endorsed to the Congress to create an improved enabling environment for cybersecurity.

3.1. Strengthen NCIAC as the convergence point for implementing cybersecurity policies and strategies

Shown in Figure 8 are the different overlapping areas of cybersecurity [43]. Various government agencies are mandated to strategize and implement plans in cybersecurity for each of the policy area shown. The policy areas also map directly to the strategies outlined in the PDP 2023-2028 where cybersecurity plays an important role. For example, socio-economic prosperity policy area contains PDP strategies pertaining to trade negotiations, development of skilled workers, and development of high-value industries such as that of cybersecurity, among others.

Figure 8. NCSP 2023-2028 Strategic Framework


Policy and Technological Control
Define proper use of technology, and policies in the use of technology to establish cybersecurity controls.
(DICT, DOST, NTC, NPC etc)
Socio-Economic Prosperity
Cybersecurity of e-Commerce and ensuring public trust in online transactions.
(NEDA, DTI, BSP, DOF, DBM, DOE, DOLE, DepEd, CHED, DFA , etc.)
National Security
Coordinated response and mitigation against threats in cyberspace, including misinformation, and threats to CII
(NSC, DND, AFP, NICA)
Cybercrime
Strategic area focused on defining, apprehending, and prosecuting criminals in cyberspace.
(CICC, DOJ, DILG, NBI, PNP, AMLCC, etc.)
POLICY, CONTROLS & CII REGULATION
CII PROTECTION
FORENSICS, PROSECUTION & LEGAL FRAMEWORK
CYBER ATTRIBUTION
NCIAC

Since cybersecurity is multi-disciplinary, many of these policy areas, including the mandate of different government agencies, overlap. Different agencies are therefore expected to coordinate with each other in implementing policies and strategies in these shared areas.

NCIAC [44] shall be the convergence point for all government agencies in implementing these policy areas and shall be the main forum for information sharing, policy coordination, and shall harmonize the different cybersecurity implementation plans of other government agencies. Through NCIAC, conflicting policy issuances between government agencies shall be addressed. NCIAC is chaired by the Executive Secretary and co-chaired by the Secretary of DICT and the National Security Adviser. DICT serves as the secretariat of NCIAC but its workforce can be expanded by personnel from organizations of the NCIAC co-chairs.

Foreseeing the increase in frequency of cybersecurity incidents, the NCIAC should be empowered to allow it to work faster and more agile. Different work groups or task forces are recommended to be created under NCIAC. These include working groups on strategic communications and incident response coordination, among others. These working groups shall be provided with the resources to efficiently perform tasks, including communications and working office spaces when necessary.

3.2. Promulgate an EO in CII Protection

The security and protection of CI and their CII are critical to the safety of a nation [45]. Critical Infrastructures are usually interdependent physically, logically, and in cyberspace. For example, many CII have the same long-distance telecommunications system that links different offices and, in some cases, their ICS. This system creates a complexity that is difficult to quantify. Regardless of the complexity, a comprehensive infrastructure of governance, people, and technological controls must be in place to protect CII. This interdependence makes it difficult to predict emerging vulnerabilities and breakdowns of CII [46].

Pending the enactment of a Critical Information Infrastructure Protection law, the DICT shall lead in the drafting of an Executive Order, for the promulgation of the President on Critical Information Infrastructure Protection with the following key features.

3.1.1. Use of risk-based approach in the identification of CII

Any organization, including regulatory agencies, other government agencies, the Congress, the judiciary, or any private institutions, can recommend enterprises to be recognized as CII. The recommendation shall be forwarded to the Secretary of the DICT. The recommendations will be collated and will be forwarded to NCIAC who will convene to discuss and recommend the approval of the CII. Ultimately, the list of CII will be approved by the President.

The NCIAC shall adopt a criteria for identifying CII, which shall include, but not limited to, those shown in the table below.

CRITERION TITLE	DESCRIPTION
1.Critical Assets	Operates or maintains national databases, power grids, water supplies, etc.
2.Economic Impact	The cost of the service disruption in terms of GDP percentage

3.Affected population / Geographical scope	Percentage of the affected population during the disruption of service
4.Public Peace and Order	The effect of the service interruption may result to public peace and order including public outcry/protest, rebellion or terrorism
5.Supply chain / Third-party dependencies	Interdependencies within (inter-sectoral) and between (cross-sectoral) other critical services
6.Continuance of national leadership	The effect of interruptions may affect effective national governance or disrupt established chains of command.
7.International Relations	The effect of the service interruptions may affect the relationship with international partners with the Philippine government
8.Disruption of public operations and service delivery	The disruption of the service will affect public daily operations (disruption of public transport, water, electricity/ energy, food supply; impeded service delivery)
9.Environmental Factors	The effect of losing command and control on facilities may lead to disastrous environmental effects (e.g. unauthorized release of water from dams, release of untreated water, and nuclear meltdown).

Companies, not entire industrial sectors, will be identified as CII. Once identified as a CII, the enterprise shall be informed by a letter signed by the chairpersons of the NCIAC. They shall undergo an onboarding process within 24 months. During the onboarding process, the enterprise shall:

1. Be given an orientation of their compliance requirements as a CII, along with the support that they can expect from the government;
2. Be given training on information security standards for its management;
3. Be assisted in setting-up and be provided with tools for information exchange and coordination among various government agencies, NCERT, and other CII.
4. Nominate or assign personnel with significant security clearance as the Cybersecurity Information Officer who shall be the main focal person between the enterprise and the network of CERT.
5. Submit a Risk Assessment and VAPT report of critical information assets to DICT. Part of the Risk Assessment is a list of critical information assets; and
6. Establish the CII organization’s CERT which can be in-house or outsourced.

The list of approved CII organizations shall be confidential and shall be kept and maintained by NCIAC. However, the risk management framework to be used to set the criteria for the identification of CII shall be made public.

NGAs, LGUs, and GOCCs may be identified as CII and shall also undergo the same onboarding process.

3.1.2 Monitor compliance of CII to cybersecurity risk reduction regulations

The following requirements shall be regularly submitted by the CII to their regulatory agency and to the DICT CSB:

1. Audit report by an external auditor, submitted every two years, on the sufficiency of governance and technological cybersecurity controls of an organization. The adopted cybersecurity standard shall be based either on an industry-accepted cybersecurity standard or those imposed by the regulatory agency to the sector. The DICT may also issue sector-specific guidelines on cybersecurity, in coordination with the industry players, the academe, and the regulatory agencies. These will be transitioned to annual reporting on the third year of implementation.
2. Annual VAPT report of identified critical information assets which may be completed with the assistance of a reputable third party company or with the DICT CSB.
3. CII Organization CERT quarterly report of issues handled, closed, and remediated.
4. Compliance to reporting requirements of the Data Privacy Act of 2012, and other relevant cybersecurity and cybercrime laws, rules, and regulations.

For Item number 1, the DICT shall coordinate with the DTI's Bureau of Philippine Standards in adopting the standard for Information Security Management Systems. The DICT-CSB recognizes the NIST Cybersecurity Framework for Critical Infrastructure as the appropriate standard to be adopted for the audit. Normative references are outlined in its Annex A such as, but not limited to, ISO 27001 Annex A and COBIT, among others [37].

In addition, the CII must accommodate all reasonable requests by the DICT CSB and/or their regulators for site inspection, access to their critical information asset records, and conduct non-intrusive VAPT to their critical information assets.

Meanwhile, the CII may be given assistance on the following:

1. Securing its facilities from security threats with the aid state forces such as the PNP and the AFP.
2. Use of Government Cybersecurity trust anchors when applicable.
3. Annually, the DICT shall coordinate cybersecurity drills, trainings, and exercises with all regulatory agencies, including some of their CII. DICT shall also prioritize the cybersecurity training of CERT personnel of CII.

3.1.3. Establish CII CERTs

Part of the onboarding process for the CII is establishing their organization CERTs. Its responsibility include:

1. Triage and classify cybersecurity incidents within the organization;
2. Respond to cybersecurity incidents;
3. For severe or critical cybersecurity incidents, coordinate the response with the NCERT and the Sector CERT;
4. Develop and manage the cybersecurity response life cycle within the organization;
5. Conduct cybersecurity tabletop simulations, drills, and exercises within the organization;

6. Promote and train the organization in adopting a cyber-safe culture.
7. Act as the primary focal person of the organization to the nationwide network of CERT.

The CII shall appoint at least a mid-level manager to be the focal person to the nationwide network of CERT. This person shall be the primary contact for communications to and from the Sector CERT and the NCERT.

While it is not mandatory, the CII may create a Security Operations Center (SOC) to monitor the security of their critical information assets.

3.3. Develop policy and capability for voluntary security labelling of IOT devices

While, in general, the security labelling scheme is voluntary, the country shall work for mandatory security labelling of routers and switches being sold in the market. To operationalize this strategy, the DICT CSB shall form a committee along with the DTI's Bureau of Philippine Standards, representatives from trade groups, and manufacturers of commonly used IOT devices, and the academe. The country shall work to harmonize its technical evaluation and conformity standards with the Common Criteria and strive to fulfill the requirements for Common Criteria Recognition Arrangement (CCRA)[8]. This will remove the need for repeating certifications for vendors who already have an assigned common criteria assurance level.

Asymmetric information potentially creates a lemon industry [47]. This is happening today for Internet of Things (IOT) products. An IOT market skew is observed in favor of cheap but non-secure products. To improve this, the public should be provided with more information about the security of the products available in the market. This is where product certification comes in. DICT should work with the DTI to create such standard which may be based on ETSI EN 303-645 [48] or other similar international standard.

Recognizing the current lack of personnel and mechanism for the Philippine government to create a technical evaluation laboratory, the labelling scheme can consider mutual recognition of other certification criteria or process, such as those employed by Singapore, UK, EU, or the US. Existing certification criteria recognized by other countries can be mapped to national IOT security labeling. Mutual recognition of technical evaluation certifications between countries is an encouraged practice .

3.4. Promulgate guidelines and procedures for accreditation of trusted VAPT service providers

There are reports of VAPT service providers who act surreptitiously to exploit found system vulnerabilities to either extort money or to earn more money. These practices are illegal. The DICT shall revise its existing Department Circular to strengthen safeguards on accreditation of VAPT service providers. These include getting feedback from the service providers' customers, instituting a complaints mechanism for performed VAPT, and ensuring VAPT service providers have both the technical knowledge and experience to provide these services.

[8] https://www.commoncriteriaportal.org/ccra/

3.5. Establish policies, guidelines and procedures for the use of trusted and secure crypto-primitives, elements and protocols

The DICT shall work with the DOST, DTI, the academe and the private sector in defining, and promoting the use of internationally recognized standards in the use of cybersecurity primitives and protocols such as, but not limited to, the use of SSL, TLS, PKI, and SDNS. The proper use of crypto primitives and cryptographic protocols shall be published as technical papers by DICT. The technical papers shall be valuable resources that take into account the evolving landscape of cybersecurity. As an example, the DICT, may seek assistance in defining what would be the nationally acceptable crypto-primitive and protocol that can be used in asymmetric key encryption used in key exchanges given that quantum computers can now theoretically use Shore's Algorithm to solve the reverse factorization problem of very large prime numbers [49]. Another example is what encryption algorithms, including key lengths would be acceptable for storing and transmitting confidential information.

3.6. Establish cybersecurity minimum standards

Proper guidance shall be given to government agencies and LGUs to allow each to adopt appropriate control measures relative to their size and budget. The DICT shall coordinate with the DTI Bureau of Philippine Standards to adopt a framework for cybersecurity. Based on the framework of the adopted cybersecurity standard for government, the DICT shall coordinate with other government instrumentalities and agencies and issue appropriate guidelines for the accepted practice for at least the following areas:

1. <u>Data classification:</u> There is a need for the government to centrally mandate a data classification system. The data classification system will also affect the asset risk assessment framework. Currently, the government classifies data along these classes: (a) confidential; (b) secret; (c) top secret; (d) restricted; and, (e) declassified [50]. Uniform rules shall apply to all government instrumentalities and LGUs in handling each type of data in storage or in transit.
2. <u>Supply Chain Security:</u> the DICT shall work with the DBM and the Government Procurement Policy Board (GPPB) in defining a standard for cybersecurity products to be procured by government agencies. The NCERT had seen many cases of compromised government data assets because these were stored in non-secure, non-certified products. The standard should consider the voluntary security certification system being proposed and should prescribe the minimum level of security certification or label based on the classification of data that will be handled. For software products, government agencies shall require a software bill of materials to determine the security of software being procured.
3. <u>Secure Software Development Lifecycle (Secure SDLC):</u> The DICT shall prescribe a standard Secure Software Development Lifecycle to be followed by government agencies and their vendors engaged in software development.
4. <u>Adopt a zero-trust policy for government:</u> the Philippine government shall additionally adopt the zero-trust architecture as a security policy for all government information assets [51].

5. Adopt a National Security-and-Privacy-by-Design Framework**:** security varies among design frameworks. The most cited is Saltzer and Schroeder's design principles contained in their 1975 paper, "The Protection of Information in Computer Systems" [52]. These design principles have underwent multiple iterations of improvement. A more modern yet good example is the US NIST security by design framework [53]. DICT shall circularize security-by-design and privacy-by-design frameworks that should be uniformly applied by all government agencies.

3.7. Propose new legislative measures to strengthen cybersecurity

The DICT shall coordinate with all government agencies and submit to the Congress the proposed Cybersecurity Act[9].

These proposed policies are aimed to solve issues of 1) misaligned incentives, (2) asymmetric information, and (3) externalities that hinder voluntary adoption of cybersecurity measures. The goal is to create a national policy framework that will promote innovation and reduce barriers to compliance in cybersecurity. The policies shall also advocate shared responsibility between the public and private sectors. The proposed laws shall apply a risk management approach in implementing cybersecurity policies and shall penalize organizations that apparently show behavior of patent neglect in protecting their critical cyberspace assets.

It should be reiterated that in the absence of a law, some of these items can still be implemented through mutual cooperation of the public and private sectors, through regulatory agencies or through DICT memorandum circulars.

3.7.1. Information sharing and mandatory disclosure of severe and critical cybersecurity incidents among government and CII

To ensure proper management of incidents at a sectoral and national scale, incidents classified as severe or critical shall be reported to NCERT and Sector CERTs. The purpose of the mandatory disclosure is to encourage and facilitate the bi-directional flow of real-time actionable intelligence to enable the network of CERTs and other NGAs in-charge of cybersecurity to assess the situation and to assist in emergency response. Regulators may not readily exact fines and other penal provisions based on mandatory disclosures, unless the breach was due to gross negligence or non-compliance.

Reports of cybersecurity incidents among government agencies and CII are classified information. Ensuring the confidentiality of the disclosure is essential to establish trust and confidence in the reporting mechanism. However, incidents that potentially compromise confidentiality, secrecy, and integrity of PII should be publicly disclosed to the NPC. SCERT and NCERT should, in compliance with the Data Privacy Act of 2012 [54], inform data subjects within 72 hours that their PII may have been exposed to allow risk mitigation. It is worth noting that the Data Privacy Act of 2012 requires organizations to submit an annual report of the summary of documented security incidents and personal data breaches to the NPC.

There is a consensus on the value of information sharing and mandatory disclosure of cybersecurity incidents [43] [14] [15] [55]. Information sharing and mandatory disclosure

[9] The proposed law is part of the legislative agenda enumerated in Chapter 13 of the PDP 2023-2028.

of cybersecurity incidents not only solve the problem of asymmetric information, but also create an incentive for responsible organizations that adopt good cybersecurity processes and technologies. Mandatory disclosure, when done right, shows economic forces freely at play, where innovations in cybersecurity will help push the entire ecosystem into responsible behavior without the need to set mandatory compliance to security standards that are rigorous, slower to adapt, and do not scale based on the unique requirements of each organization.

3.7.2. Create a safe environment for security researchers to responsibly disclose cybersecurity incidents

The new proposed cybersecurity law(s) shall provide legal protection to any security researcher disclosing a vulnerability found in any asset in cyberspace, whether from a private enterprise or from a government agency. The term "responsible disclosure" shall be defined in the proposed law.

This rule shall also apply to government agencies and government workers. Thus, the DICT, through the CSB, shall perform periodic VAPT scans on any cyberspace asset it finds with an IP address or AS assigned to the Republic of the Philippines. Any vulnerability found for any asset shall be reported directly to the cyberspace asset owners.

While the threat landscape is continuously evolving, responsible actors in cyberspace must update both their information and skills with agility to match the speed by which threat actors identify vulnerabilities and exploit them. Public policy must be geared to favor incentivizing individuals and/or organizations that assist in securing cyberspace. These include security researchers.

Concluding Notes: Operationalizing the NCSP 2023-2028

The NCSP 2023-2028 is the cybersecurity masterplan of the country. It is aligned to the PDP 2023-2028. Each agency, however should develop their own cybersecurity or cybercrime strategies consistent with the NCSP and, ultimately, to the PDP.

The results matrix, as shown in Table 1, is not exhaustive and should be revisited based on developing trends and discussions with other government agencies.

Table 1. NCSP 2023-2029 Results Matrix

Results	**Targets**							**Responsible Agency**
	Base	**2023**	**2024**	**2025**	**2026**	**2027**	**2028**	
Contribution of e-Commerce to GDP increased (%)	1.7	TBD	TBD	TBD	TBD	TBD	TBD	DTI (please refer to PDP)
Percentage of cyber incident reports processed and or closed and remediated	80%	Increasing annually						DICT (please refer to PDP)

Results	Targets							Responsible Agency
	Base	2023	2024	2025	2026	2027	2028	
GCI ranking (vs ASEAN) increased	6th	6th	6th	5th	5th	4th	4th	DICT
Cybersecurity incident resolution time decreased (days)	30	Decreasing annually						DICT
CII onboarded, managed	0	TBD	TBD	TBD	TBD	TBD	TBD	DICT, NCIAC
CERTS in NGAs established (%)	1%	1%	25%	50%	75%	100%	100%	DICT
CERTs of provincial level LGUs with established (%)	0%	TBD	TBD	TBD	TBD	TBD	TBD	DILG
National Intelligence Coordinating Network Established				100%				NICA
DND and AFP CERTs established				100%				DND
Number of HEIs offering Cybersecurity curriculum	3	7	25	TBD	TBD	TBD	TBD	CHED
Cybersecurity professionals with certifications increased	TBD	TBD	TBD	TBD	TBD	TBD	TBD	DICT, TESDA
Secure inter-domain Routing protocol among ISPs implemented					100%			NTC, DICT
National Cybersecurity Training and Research Center established					100%			CHED, DICT, DOST

There are two major legislative items supported by the NCSP 2023-2028. These legislative agenda are also found in Chapter 13 of the PDP 2023-2028. They are: (1) the Critical Information Infrastructure Protection Act (CIIPA) and (2) the Cybersecurity Act. The responsible agency for both shall be DICT. Other legislative agenda enumerated in the PDP that relates to e-Governance, e-Commerce, and peace and security should also have provisions to strengthen cybersecurity using the NCSP 2023-2028 as reference.

###

References

[1] *Information technology - Security techniques - Guidelines for cybersecurity*, I. S. O. (ISO), Switzerland, 2012.

[2] *Information Technology Security Techniques - Information Security Management Systems Requirements (ISO/IEC 27001:2013)*, B. S. Institution, Janiuary 26, 2017 2017.

[3] K.-P. Saalbach, "Attribution of Cyber Attacks," in *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace*, C. Reuter Ed. Wiesbaden: Springer Fachmedien Wiesbaden, 2019, pp. 279-303.

[4] "An act creating the department of information and communications technology, defining its powers and functions appropriating funds therefor, and for other purposes," ed. Philippines, 2016.

[5] (2023). *Philippine Development Plan 2023-2028*. [Online] Available: https://pdp.neda.gov.ph/philippine-development-plan-2023-2028/

[6] *Recommendation ITU-T X.125 Overview of Cybersecurity*, I. T. U. (ITU), 2008. [Online]. Available: https://www.itu.int/rec/T-REC-X.1205-200804-I

[7] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining Cybersecurity," *Technology Innovation Management Review,* vol. 4, no. 10, 2014. [Online]. Available: http://timreview.ca/article/835.

[8] S. N. Romaniuk and M. Manjikian, Eds. *Routeledge Companion to Global Cybersecurity Strategy*. New York: Routeledge, 2021.

[9] B. Reyes, "Kaspersky: Philippines Ranked 4th Worldwide With Most Number of Web Threats," in *Manila Bulletin*, ed. Manila, Philippines: Manila Bulletin, 2022.

[10] Country's Digital Transactions Reached PhP 1.87 Trillion in 2021, with 9.6 Percent Contribution to the Gross Domestic Product [Online] Available: https://psa.gov.ph/digital-economy

[11] Department of Trade and Industry. (2022). *Basta e-Commerce Madali 2022*. [Online] Available: https://ecommerce.dti.gov.ph/madali/mapped.html

[12] "The Philippine IT-BPM Industry Roadmap 2028 Executive Summary," IT & Business Process Association of the Philippines, Manila, 2022. [Online]. Available: https://www.ibpap.org/knowledge-hub/research

[13] A. P. H. Fabe and E. Zarcilla-Genecella, "The Philippines' cybersecurity strategy: strenghening partnerships to enhance cybersecurity capability," in *Routeledge companion to global cyber-security strategy (kindle edition)*, S. N. Romaniuk and M. Manjikian Eds. New York: Routeledge, 2021, ch. 26.

[14] T. Moore, "The economics of cybersecurity: Principles and policy options," *International Journal of Critical Infrastructure Protection,* vol. 3, no. 3, pp. 103-117, 2010/12/01/ 2010, doi: https://doi.org/10.1016/j.ijcip.2010.10.002.

[15] J. J. Cordes, "An Overview of the Economics of Cybersecurity and Cybersecurity Policy," *CSPRI Report,* pp. 1-18, 2011.

[16] M. Söllner, A. Hoffmann, and J. M. Leimeister, "Why different trust relationships matter for information systems users," *European Journal of Information Systems,* vol. 25, no. 3, pp. 274-287, 2016/05/01 2016, doi: 10.1057/ejis.2015.17.

[17] B. van den Berg and E. Keymolen, "Regulating security on the Internet: control versus trust," *International Review of Law, Computers & Technology,* vol. 31, no. 2, pp. 188-205, 2017/05/04 2017, doi: 10.1080/13600869.2017.1298504.

[18] N. Luhmann, "Familiarity, confidence, trust: Problems and alternatives," *Trust: Making and breaking cooperative relations,* vol. 6, no. 1, pp. 94-107, 2000.

[19] L. Coles-Kemp, D. Ashenden, #039, and K. Hara, "Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen," *2018,* cybersecurity; cyberspace; power; social contract; sovereignty vol. 6, no. 2, p. 8, 2018-06-11 2018, doi: 10.17645/pag.v6i2.1333.

[20] E. D. Borghard and S. W. Lonergan, "Confidence Building Measures for the Cyber Domain," *Strategic Studies Quarterly,* vol. 12, no. 3, pp. 10-49, 2018. [Online]. Available: http://www.jstor.org/stable/26481908.

[21] G. A. Crowther, "The Cyber Domain," *The Cyber Defense Review,* vol. 2, no. 3, pp. 63-78, 2017. [Online]. Available: http://www.jstor.org/stable/26267386.

[22] S. Goel and B. Nussbaum, "Attribution across cyber attack types: network intrusions and information operations," *IEEE Open Journal of the Communications Society,* vol. 2, pp. 1082-1093, 2021.

[23] *Guidelines on Security and Privacy in Public Cloud Computing,* NIST, Washington DC, USA, 2011.

[24] O. Çetin *et al.*, "Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai," in *NDSS*, 2019.

[25] M. Eeten, J. Bauer, H. Asghari, S. Tabatabaie, and D. Rand, "The Role of Internet Service Providers in Botnet Mitigation an Empirical Analysis Based on Spam Data," 08/15 2010.

[26] A. Noroozian, E. T. Rodriguez, E. Lastdrager, T. Kasama, M. V. Eeten, and C. H. Gañán, "Can ISPs Help Mitigate IoT Malware? A Longitudinal Study of Broadband ISP Security Efforts," in *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*, 6-10 Sept. 2021 2021, pp. 337-352, doi: 10.1109/EuroSP51992.2021.00031.

[27] "Cybercrime Prevention Principles for Internet Service Providers," World Economic Forum, Geneva, Switzerland, 2020. [Online]. Available: https://www3.weforum.org/docs/WEF_Cybercrime_Prevention_ISP_Principles.pdf

[28] K. Butler, T. R. Farley, P. McDaniel, and J. Rexford, "A survey of BGP security issues and solutions," *Proceedings of the IEEE,* vol. 98, no. 1, pp. 100-122, 2009.

[29] A. Mitseva, A. Panchenko, and T. Engel, "The state of affairs in BGP security: A survey of attacks and defenses," *Computer Communications,* vol. 124, pp. 45-60, 2018/06/01/ 2018, doi: https://doi.org/10.1016/j.comcom.2018.04.013.

[30] *RFC 7454: BGP Operations and Security*, IETF, December 20, 2018 2018. [Online]. Available: https://datatracker.ietf.org/doc/rfc7454/

[31] *Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation,* NIST, Washington DC, USA, 2019.

[32] *Resilient Interdomain Traffic Exchange: BGP Security and DDOS Mitigation*, NIST, Washington DC, USA, 2019.

[33] UNESCO, "Internet for trust - Towards guidelines for regulating digital platforms for information as a public good," Paris, 2023. Accessed: July 1, 2023. [Online]. Available: https://unesdoc.unesco.org/ark:/48223/pf0000384031

[34] P. Meyer and S. Métille, "Computer security incident response teams: are they legally regulated? The Swiss example," *International Cybersecurity Law Review,* vol. 4, no. 1, pp. 39-60, 2023/03/01 2023, doi: 10.1365/s43439-022-00070-x.

[35] M. J. West-Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, and R. Ruefle, "Handbook for computer security incident response teams (CSIRTs)," CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2003.

[36] R. Ruefle, A. Dorofee, D. Mundie, A. D. Householder, M. Murray, and S. J. Perl, "Computer Security Incident Response Team Development and Evolution," *IEEE Security & Privacy,* vol. 12, no. 5, pp. 16-26, 2014, doi: 10.1109/MSP.2014.89.

[37] *Framework for Improving Critical Infrastructure Cybersecurity version 1.1,* NIST, Washington DC, USA, April 16, 2018 2018.

[38] APTelecom, "Submarine Cable Infrastructure: Maintenance and Repair Analysis: South East Asia," APTelecom, 2023.

[39] P. Meyer, "Norms of Responsible State Behaviour in Cyberspace," in *The Ethics of Cybersecurity*, M. Christen, B. Gordijn, and M. Loi Eds. Cham: Springer International Publishing, 2020, pp. 347-360.

[40] WEF and Accenture, "Global Cybersecurity Outlook 2023: Insight Report," 2023. [Online]. Available: https://www.weforum.org/reports/global-cybersecurity-outlook-2023

[41] "Conferring Civil Service Eligibility on Electronic Data Processing (EDP) Specialists on the Bases of Their Qualifications and the Requirements of the Public Service," in *PD 1408,* ed. Philippines, 1978.

[42] "An act to enhance the philippine digital workforce competitiveness, establishing for the purpose an inter-agency council for development and competitiveness of philippine digital workforce and for other purposes," ed. Philippines, 2022.

[43] OECD, "OECD Policy Framework on Digital Security," 2022. [Online]. Available: https://www.oecd-ilibrary.org/content/publication/a69df866-en

[44] "Reorganizing the National Cybersecurity Inter-Agency Committee, Amending Executive Order No. 189 (S. 2015) And for Other Purposes," in *Executive Order 95 s. 2019,* ed. Philippines, 2019.

[45] C. Alcaraz and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century," *International Journal of Critical Infrastructure Protection,* vol. 8, pp. 53-66, 01/31 2015, doi: 10.1016/j.ijcip.2014.12.002.

[46] E. Zio, "Critical Infrastructures Vulnerability and Risk Analysis," *European Journal for Security Research,* vol. 1, 10/01 2016, doi: 10.1007/s41125-016-0004-2.

[47] V. Garg, "A Lemon by Any Other Label," *ICISSP,* pp. 558-565, 2021.

[48] *ETSI EN 303 645 v.2.1.1 CYBER; Cyber Security for Consumer Inrternet of Things: Baseline Requirements*, ETSI, 2020. [Online]. Available: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[49] D. Gollman, "Foundations of Computer Security," in *Computer Security,* 3rd ed. West Sussex, United Kingdom: John Wiley & Sons, 2011, ch. 3.

[50] "Promulgating rules governing security of classified matter in government offices," in *Memorandum Circular No. 78 series of 1964, Office of the President*, ed. Republic of the Philippines, 1964.

[51] *NIST SP 800-207: Zero Trust Architecture*, NIST, Washington DC, USA, 2020.

[52] R. Smith, "A Contemporary Look at Saltzer and Schroeder's 1975 Design Principles," *Security & Privacy, IEEE,* vol. 10, pp. 20-25, 11/01 2012, doi: 10.1109/MSP.2012.85.

[53] *Engineering Trustworthy Secure Systems*, NIST, Washington DC, USA, 2022. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-160v1r1

[54] "An act protecting individual personal information in information and communications systems in the government and the private sector, creating for this purpose a national privacy commission, and for other purposes," ed. Republic of the Philippines, 2012.

[55] N. Jentzsch, "State-of-the-Art of the Economics of Cyber-Security and Privacy," in "IPACSO Deliverable d4.1," February 1, 2016 2016. [Online]. Available: https://ssrn.com/abstract=2671291