DEPARTMENT CIRCULAR NO. DC 2025-01-0001

INSTITUTIONALIZING THE ENERGY SECTOR CYBERSECURITY AND CYBER RESILIENCE FRAMEWORK

WHEREAS, Republic Act (RA) No. 7638 or the *"Department of Energy (DOE) Act of 1992"* declares the policy of the State to ensure a continuous, adequate, and economic supply of energy with the end in view of ultimately achieving self-reliance in the country's energy requirements;

WHEREAS, Section 4 of RA 7638 provides that the DOE shall prepare, integrate, coordinate, supervise, and control all plans, programs, projects, and activities of the Government relative to energy exploration, development, utilization, distribution, and conservation;

WHEREAS, Section 2 of RA 10173 or the *"Data Privacy Act of 2012"* declares that the State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems (ICT) in the government and private sector are secured and protected;

WHEREAS, Section 2 of RA 10175, or the *"Cybercrime Prevention Act of 2012"* declares that the State recognizes the importance of providing an environment conducive to the development, acceleration, and rational application and exploitation of ICT to attain free, easy, and intelligible access to exchange and/or delivery of information;

WHEREAS, Section 5 of RA 10844, or the *"Department of Information and Communications Technology Act of 2015"* (DICT Act), mandates the DICT as a policy, planning, coordinating, implementing, and administrative entity of the Executive Branch of the government that will plan, develop, and promote the national ICT development agenda;

WHEREAS, Chapter 5 of the Philippine Grid Code (2016 Edition) provides the requirements for the interconnection between power generation facilities to the Grid and its Supervisory Control and Data Acquisition (SCADA) System wherein a Remote Terminal Unit (RTU) is used for interconnection with the System Operator's Control Center to serve as telemetry equipment for monitoring real-time information and controlling the equipment at the user system;

WHEREAS, Section 3 of RA 11659 or *"An Act Amending Commonwealth Act No. 146, Otherwise Known as the Public Service Act, As Amended"* provides that all references to the Public Service Commission in Commonwealth Act No. 146, as amended, shall pertain to any Administrative Agency to which the powers and duties of the Public Service Commission were transferred by subsequent laws, such as but not limited to (c) the Department of Energy;

WHEREAS, Section 4 of RA 11659 defined Public Utility as public service that operates, manages, or controls for public use any of the following: (1) Distribution of Electricity; (2) Transmission of Electricity; and (3) Petroleum and Petroleum Products Pipeline Transmission Systems, among others. Further, said Section provides that all concessionaires, joint ventures, and other similar entities that wholly operate, manage, or control for public use in the sectors listed above are public utilities;

WHEREAS, Section 29 of RA 11659 provides that Administrative Agencies must ensure the annual conduct of performance audit by an independent evaluation team to monitor cost, the quality of services provided to the public, and the ability of the public service provider to immediately and adequately respond to emergency cases. Provided that in the case of critical infrastructure and public utilities, the performance audit shall include risk assessment, emergency response, and cybersecurity, among others. Metrics for various types of services must be established to sustain the reliability, security, and safety of the public;

WHEREAS, Section 7.1 of DOE Department Circular (DC) No. DC2018-01-0001, titled *"Adoption of Energy Resiliency in the Planning and Programming of the Energy Sector to Mitigate Potential Impacts of Disasters",* created the Task Force on Energy Resiliency (TFER) which is the primary organization activated to respond to natural (typhoons, earthquakes, floods, volcanic eruptions, landslides, fires, among others) and human-induced disasters (bombing, global oil supply, and peace disruption, among others) to ensure immediate restoration of power and oil supply and services in disaster-stricken areas;

WHEREAS, Section 2.1. (d) of DOE DC No. DC2022-06-0028, titled *"Supplementing Department Circular No. DC2018-01-0001 on the Energy Resiliency Planning and Programming of the Energy Sector and on Task Force on Energy Resiliency (TFER) Functions and Structure to Mitigate Impacts of Disasters",* mandates the TFER to develop and improve preparedness measures, operational and coordination mechanisms as well as strengthen organizational capacities and practices to mitigate disaster effects and ensure expeditious restoration of energy supply during and in the aftermath of disruptive events;

WHEREAS, DOE DC No. DC2020-02-0003, titled *"Providing a National Smart Grid Policy Framework for the Philippine Electric Power Industry and Roadmap for Distribution Utilities",* states that to prevent potential cyber-attacks/breaches during Smart Grid deployments, Generation Companies (GenCos), Transmission Network Providers (TNPs), and Distribution Utilities (DUs) shall develop a cybersecurity infrastructure and ensure cost-effective protection, compliant with all relevant laws and regulations as well as internationally accepted standards at the appropriate level of adoption and application;

WHEREAS, Chapter 13.1 of the Philippine Development Plan 2023-2028 recognizes peace and security as an essential foundation of sustainable development; and while the government remains committed to pursuing peace by mainstreaming peacebuilding, formulating the National Cybersecurity Plan (NCSP), and activating the National Computer Emergency Response Team (NCERT) and the National Cybersecurity Operations Center, a more concerted effort in cybersecurity is still needed;

WHEREAS, the strategies for achieving cybersecurity include developing a manual of operations and standard protocols on cybersecurity for public and private institutions, adopting a legal framework to strengthen cybersecurity, establishing policies on minimum information security standards to protect critical information infrastructure (CII) and the ICT systems of public institutions, transportation, and e-commerce transactions, as well as increasing the capacity of the private sector to mitigate piracy of creative outputs;

WHEREAS, Chapter 3 of the National Security Policy (NSP) 2023-2028 emphasizes the Philippines' commitment to fostering the sustainable growth of a digital economy. It also highlights the need to protect online users and maintain an open and secure cyberspace in the country. In terms of energy security, the policy addresses the importance of safeguarding critical energy infrastructures against the impacts of climate change and human-induced hazards;

WHEREAS, the NCSP 2023-2028 has been adopted through the issuance of Executive Order (EO) No. 58 s. 2024 by President Ferdinand R. Marcos Jr. and directed the adoption, alignment, and implementation of the NCSP 2023-2028 as the whole-of-nation roadmap for the integrated development and strategic direction of the country's cybersecurity;

WHEREAS, one of the core principles declared in the NCSP 2023-2028 states that the Philippine Government, its citizens, and the public and private sectors have a shared responsibility for cybersecurity. Furthermore, all government agencies are encouraged to develop and improve their cybersecurity strategies and sub-plans that are consistent with the NCSP 2023-2028;

WHEREAS, the Philippine Energy Plan (PEP) 2023-2050, specifically on the Resiliency and Security of Energy Infrastructures (Volume III), acknowledges that the security of energy infrastructure and facilities, apart from resiliency, is also a paramount concern to support the growth of the economy. Hence, keeping the energy supply chain fully functional and protected from human-induced hazards is among the primary agendas of the government through the national security agencies;

WHEREAS, electricity plays an important role in transitioning the sector to the Fourth Industrial Revolution (Industry 4.0), which utilizes the Internet of Things (IoT), Artificial Intelligence (AI), cloud computing, and digital platforms in key manufacturing industries such that by the end of the planning period, it accounts for 53.6 percent of the sector's total energy requirement.

WHEREAS, the increasing reliance on digital technologies in the energy sector necessitates robust cybersecurity measures to safeguard Information Technology (IT) and Operational Technology (OT) infrastructure, including interconnected systems between government offices, power sector stakeholders, oil and gas industry participants, and other government agencies to ensure the confidentiality, integrity, availability, non-repudiation, and authentication of information and data stored within these systems, protecting them from all forms of misuse, abuse, and illegal access, and recognizing the critical need for fail-safe mechanisms to guarantee the continued and reliable operation of the energy grid in the event of a cyberattack;

WHEREAS, a writeshop was carried out on 20 May 2024 to facilitate the formulation of a Department Circular on the Cybersecurity Energy Policy and to conduct a thorough review of the provisions thereof. A comprehensive public consultation was subsequently held on 27 and 28 June 2024 for Energy Stakeholders and Participants, Government Agencies, and DOE Personnel, as well as for Government Agencies and DOE Personnel respectively. During said public consultations, the provisions of the Draft Department Circular on Cybersecurity Energy Policy were meticulously refined and rigorously reviewed by distinguished experts in their respective fields;

NOW, THEREFORE, premises considered, the DOE hereby promulgates the adoption of this policy ***"Institutionalizing the Energy Sector Cybersecurity and Cyber Resilience Framework"*** by the concerned energy sector stakeholders and participants in collaboration with other government and non-government agencies.

SECTION 1: SCOPE AND APPLICABILITY

The policy shall apply to all energy industry stakeholders and participants, which includes, but are not limited to, energy resources, power (including generation, transmission, and distribution), the oil and gas industry, and the utilization sector identified or classified as CII.

SECTION 2: GENERAL POLICIES AND PRINCIPLES

2.1 This policy shall adhere to the following guiding principles aligned with the NCSP 2023-2028 and other existing government plans, policies, laws, and regulations to ensure cybersecurity and cyber resilience of CIIs in the energy sector, specifically:

2.1.1 **Supports the national goals on cybersecurity.** Adheres to the vision of desired national goals of a trusted, secure, and reliable cyberspace as stipulated under the NCSP 2023-2028;

2.1.2 **Establishes governance and compliance with policies and standards.** Ensures adherence to plans, policies, regulations, and internationally and locally recognized standards to manage and mitigate cybersecurity risks of CIIs;

2.1.3 **Enhances cybersecurity measures.** Implements robust cybersecurity measures and practices to protect, safeguard, and strengthen the IT and OT infrastructures including interconnected systems of all energy industry stakeholders and participants against cyber risks and hazards;

2.1.4 **Ensures cyber resilience.** Develops the capacity of IT and OT infrastructures to withstand and rapidly recover from severe and critical cyber incidents that may hamper and cause disruptions in the delivery of power, and oil and gas supply and services;

2.1.5 **Promotes collaboration and information sharing.** Fosters a culture of collaboration and facilitates information sharing among government agencies and energy stakeholders to increase organizational capacity and address cyber threats through early detection, prevention, and coordinated response to cyber-attacks;

2.1.6 **Increases the cybersecurity professionals and expertise.** Develops and improves preparedness measures, coordination mechanisms, and organizational capacities through cybersecurity training, education, and awareness;

2.1.7 **Adopts an Information Security Framework.** Anchors to the pillars of information security such as Confidentiality, Integrity, Availability, Non-Repudiation, Authenticity, Privacy, and Safety (CIANA-PS) in cyberspace to attain the objectives of the NCSP; and

2.1.8 **Promotes investments in cybersecurity.** Formulates comprehensive and adaptable financial and investment policies that consider consumer welfare to encourage investments in cybersecurity and cyber resilience programs of organizations.

SECTION 3: DEFINITION OF TERMS

a) **Authenticity** - refers to the property that an entity is what it claims to be. (NCSP 2023-2028)

b) **Availability** - refers to the property of being accessible and usable upon demand by an authorized entity. (NCSP 2023-2028)

c) **Confidentiality** - refers to the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. (NCSP 2023-2028)

d) **Critical Infrastructure (CI)** - refers to 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. (NCSP 2023-2028)

It also refers to any public service that owns, uses, or operates systems and assets, whether physical or virtual, so vital to the Republic of the Philippines that the incapacity or destruction of such systems or assets would have a detrimental impact on national security, including telecommunications and other such vital services as may be declared by the President of the Philippines. (RA 11659)

e) **Critical Information Infrastructure (CII)** - refers to the information process and Information Communications Technology that form part of the operation of the Critical Infrastructures (CI). (NCSP 2023-2028)

In the energy sector, CII includes both the Information Technology (IT) and Operational Technology (OT) systems and assets, both physical and digital, that are essential for the reliable and secure operation of the energy supply and services, including power, oil and gas, and the utilization sector.

f) **Cyber** - refers to a computer or a computer network, the electronic medium in which online communication takes place. (RA 10175)

g) **Cybercrime** - refers to criminal offenses committed on the internet or aided by the use of computer technology. (NIST Computer Security Resource Center Glossary)

h) **Cyber Resilience** - refers to the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. (NIST SP 800-172)

i) **Cybersecurity** - refers to the organization and collection of resources, processes, and structures to preserve Confidentiality, Integrity, Availability, Non-Repudiation, Authenticity, Privacy, and Safety (CIANA-PS) in cyberspace. (NCSP 2023-2028)

It also refers to the collection of tools, policies, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment, and the organization and user's assets. (RA 10175)

j) **Cybersecurity Incident** - refers to 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). (NCSP 2023-2028)

k) **Data Sharing Agreement (DSA)** - is a formal contract between two or more entities that outlines the terms and conditions under which data can be shared. This agreement ensures that the data being shared is protected and that both parties comply with relevant legal and regulatory requirements, particularly those set forth by the Data Privacy Act of 2012 (RA 10173). The DSA details the purpose of data sharing, the types of data to be shared, the responsibilities of each party, data security measures, and compliance with data protection laws. (RA 10173)

l) **Energy Resiliency** - refers to the ability and quality that enables energy systems to withstand extreme natural and manmade disasters, to recover and return to normal conditions in a timely and efficient manner, and to build back better, thereby securing a stable energy supply to society and reducing negative impacts on human lives and economic activities from energy supply disruption. (APEC Energy Resiliency Principle)

m) **Energy Sector** - refers to energy industry participants in the energy resource, renewable energy, power (generation, transmission, and distribution), oil, gas, and energy utilization sectors, among others.

n) **Industrial Control System (ICS)** - refers to the general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy). (NIST SP 800-37 Rev.2)

o) **Information Technology (IT)** - refers to any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage,

manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. (NIST SP 800-39)

p) **Information Security** - refers to the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability. (NIST SO 800-59)

q) **Industrial Internet of Things (IIoT)** - refers to the sensors, instruments, machines, and other devices that are networked together and use internet connectivity to enhance industrial and manufacturing business processes and applications. (NIST SP 800-172)

r) **Internet of Things (IoT)** - refers to the network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information. (NIST SP 800-172 and NIST SP 800-172A)

s) **Integrity** - refers to the property of accuracy and completeness. (NCSP 2023-2028)

t) **NCERT-PH** - refers to the official name of the Philippine National Computer Emergency Response Team (NCSP 2023-2028). NCERT-PH or Computer Security and Incident Response Team (CSIRT) refers to "an organization that studies computer and network security in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and to offer other information to help improve computer and network security". At present, "both terms (NCERT-PH and CSIRT) are used in a synonymous manner." (ENISA, 2015 and ENISA, 2015a)

u) **Non-Repudiation** - refers to the ability to prove the occurrence of a claimed event or action and its originating entities. (NCSP 2023-2028)

v) **Operational Technology (OT)** - refers to programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems (ICS), building management systems, fire control systems, and physical access control mechanisms. (NIST SP 800-37 Rev. 2)

w) **Personal Information** - refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably or directly ascertained by the entity holding the information, or when put together with other information, would directly and certainly identify an individual. (RA 10173)

x) **Privacy** - refers to having personal control over personal information. (NCSP 2023-2028)

y) **Public Service** - refers to every individual, co-partnership, association, corporation, or joint-stock company, whether domestic or foreign, their lessees, trustees, or receivers appointed by any court whatsoever, or any municipality, province, or other department of the Government of the Philippines, that now or hereafter may own, operate, manage, or control in the Philippines, for hire or compensation, any common carrier, railroad, street railway, traction railway, subway, freight and/or passenger motor vehicles, with or without fixed route, freight or any other car service, express service, steamboat or steamship line, ferries, small water craft, such as lighters, pontines, lorchas, and others, engaged in the transportation of passengers or cargo, shipyard, marine railway, marine repair shop, public warehouse, wharf, or dock not under the jurisdiction of the Insular Collector of Customs, ice, refrigeration, canal, irrigation, pipe line, gas, electric light, heat, power, water, oil, sewer, telephone, wire or wireless, telegraph system, plant or equipment, and broadcasting stations, when owned, operated, managed, or controlled for public use or service within the Philippines, whether the owner or operator be an individual, co-partnership, association, corporation or joint-stock company, either domestic or foreign, or a trustee or receiver appointed by any court whatsoever, or any municipality, province, or other department of the Government of the Philippines, or any other entities. (Commonwealth Act No. 146 as amend)

z) **Public Utility** - refers to a public service that operates, manages, or controls for public use any of the following: (1) Distribution of Electricity; (2) Transmission of Electricity; (3) Petroleum and Petroleum Products Pipeline Transmission Systems; (4) Water Pipeline Distribution Systems and Wastewater Pipeline Systems, including sewerage pipeline systems; (5) Seaports; and (6) Public Utility Vehicles. Concessionaires, joint ventures and other similar entities that wholly operate, manage or control for public use the sectors above are public utilities. Furthermore, no other person shall be deemed a public utility unless otherwise subsequently provided by law. (Commonwealth Act No. 146, as amended by RA 11659)

aa) **Resiliency** - refers to the ability of a system, community, or society exposed to hazards to resist, absorb, accommodate, and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions. (UNDRR)

bb) **Risk** - refers to the potential loss of confidentiality, integrity, or availability of information, data, or information systems and reflects the potential adverse impacts on organizational operations, assets, individuals, other organizations, and the nation. (NCSP 2023-2028)

cc) **Safety** - refers to the expectation that a system does not, under defined conditions, lead to a state in which human life, health, property, or the environment is endangered (NIST Special Publication 800-160 Volume 1). It also refers to the freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. (NIST Special Publication 800-160, Volume 2)

dd) **Threat** - refers to the potential cause of an unwanted incident, that may result in harm to a system, individual, or organization. (NCSP 2023-2028)

ee) **Utilization Sector** - refers to the end-users or consumers of energy such as the transport, household, industry, services, and agriculture sectors. (Philippine Energy Plan 2023-2050)

ff) **Vulnerability** - refers to the weakness of an asset or control that can be exploited by one or more threats. (NCSP 2023-2028)

SECTION 4: ORGANIZATION AND MANDATE

4 This section outlines the provisions for the establishment of the Oversight Committee on Energy Sector Cybersecurity and Cyber Resilience (OC-ESCCR), the Energy Sector Computer Emergency Response Team (ES-CERT-PH), and the Technical Working Group on the Identification of Critical Information Infrastructure (TWG-IDCII). ***(Please see Annex A for the Organizational Structure)***

4.1 **Creation of an Oversight Committee on Energy Sector Cybersecurity and Cyber Resilience (OC-ESCCR)**. An Oversight Committee on ESCCR is hereby created to oversee and ensure the implementation of this policy. This Committee shall be responsible for the review, implementation, and monitoring of the policies, plans, and programs to ensure the goals and objectives on cybersecurity and resilience of the energy sector are achieved in consonance with the NCSP 2023-2028 and other relevant policies, laws, and regulations.

4.1.1 **Composition of the OC-ESCCR**. The Oversight Committee shall be led by the DOE and headed by the Energy Secretary or his/her designated Undersecretary as the Chairperson and the DICT Secretary or his/her designated Undersecretary as the Co-Chairperson.

It shall be composed of the following government agencies, attached and cooperating agencies, as well as energy sector stakeholders and participants from the power and oil & gas sectors, and other relevant government agencies/entities:

4.1.1.1 **DOE Attached Agencies**

4.1.1.1.1 National Electrification Administration (NEA)
4.1.1.1.2 National Power Corporation (NPC)
4.1.1.1.3 National Transmission Corporation (TransCo)
4.1.1.1.4 Power Sector Assets and Liabilities Management Corporation (PSALM)
4.1.1.1.5 Philippine National Oil Company (PNOC) and its Subsidiaries (PNOC Exploration Corporation and PNOC Renewables Corporation)

4.1.1.2 **Power Sector Stakeholders**

4.1.1.2.1 Independent Electricity Market Operator of the Philippines (IEMOP)
4.1.1.2.2 Philippine Electricity Market Corporation (PEMC)

4.1.1.2.3 National Grid Corporation of the Philippines (NGCP)
4.1.1.2.4 Philippine Independent Power Producers Association, Inc. (PIPPA) and Selected Members
4.1.1.2.5 Philippine Electric Plant Owners Association (PEPOA) and Selected Members
4.1.1.2.6 Philippine Rural Electric Cooperatives Association, Inc. (PHILRECA)
4.1.1.2.7 Selected Private Distribution Utilities (PDUs)

4.1.1.3 **Oil and Gas Sector Industry Participants**

4.1.1.3.1 Philippine Institute of Petroleum (PIP) and Selected Members
4.1.1.3.2 Independent Philippine Petroleum Companies Association (IPPCA) and Selected Members
4.1.1.3.3 LPG Associations Recognized by the DOE as Training Organization pursuant to the LPG Industry Regulation Act

4.1.1.4 **Other Government Agencies/Entities**

4.1.1.4.1 Energy Regulatory Commission (ERC)
4.1.1.4.2 Department of Information and Communications Technology (DICT) and its Attached Agencies - National Telecommunications Commission (NTC), National Privacy Commission (NPC), and Cybercrime Investigation and Coordinating Center (CICC)
4.1.1.4.3 National Intelligence Coordinating Agency (NICA)
4.1.1.4.4 National Security Council (NSC) Secretariat
4.1.1.4.5 Armed Forces of the Philippines (AFP)
4.1.1.4.6 Law enforcement agencies such as the Philippine National Police (PNP), National Bureau of Investigation (NBI), and Department of Justice (DOJ), as necessary for the prosecution of Cybercrimes

4.1.1.5 The OC-ESCCR may invite other government instrumentalities, private entities/organizations, academic institutions, development partners, or affected stakeholders from the agency sectors, as may be deemed necessary, to attain the objectives of this Circular.

4.1.1.6 The members and representatives of the Oversight Committee shall be prioritized and be given a period to undergo training and certifications as necessary to acquire appropriate and sufficient knowledge and skills on Cybersecurity to effectively perform the roles and functions of the ESCCR, as prescribed in Section 4.1.2.

4.1.2 **Key Functions, Roles, and Responsibilities of the Oversight Committee on ESCCR**. Establishing an Oversight Committee is critical in implementing the Philippine Energy Sector Cybersecurity and Cyber Resilience Framework. This Oversight Committee plays a pivotal role and is responsible for overseeing the cybersecurity posture of the energy

sector. It also ensures compliance with relevant laws and regulations, and fosters a culture of cybersecurity and cyber resilience through its defined functions performed based on the approved Committee Rules of Procedure. The Committee shall have the following functions:

4.1.2.1 **Strategic Oversight and Leadership**. The Oversight Committee shall provide strategic direction and leadership for cybersecurity and cyber resilience initiatives within the energy sector. It shall ensure that energy sector cybersecurity plans, policies, and programs align with the Philippine Development Plan (PDP), the National Security Policy (NSP), the Philippine Energy Plan (PEP), NCSP, and other relevant policies, laws, and regulations. As a strategy, the Oversight Committee shall:

4.1.2.1.1 Coordinate with the National Cybersecurity Inter-Agency Committee (NCIAC) on the development and implementation of policies and programs of the energy sector on cybersecurity and cyber resilience; and

4.1.2.1.2 Establish international collaboration and cooperation to enhance the governance, policies, and implementation of cybersecurity.

4.1.2.2 **Policy Development and Enforcement.** The Oversight Committee shall be responsible for developing, implementing, and enforcing cybersecurity policies, laws, regulations, and standards, specifically:

4.1.2.2.1 Recommend policies, laws, and regulations for development and/or adoption by the CIIs;

4.1.2.2.2 Ensure that these policies comply with RA 10173 (Data Privacy Act), RA 10844 (DICT Act), and other relevant regulations and internationally and locally recognized standards (i.e. ISO/IEC 27001, IEC 62443, NIST CSF, among others);

4.1.2.2.3 Review and establish the acceptable and prescribed cybersecurity minimum standards to be adopted by the energy sector CIIs;

4.1.2.2.4 Ensure the proper implementation of the protocols and mechanisms for information and threat intelligence sharing;

4.1.2.2.5 Recommend relevant research studies on cybersecurity and cyber resilience; and

4.1.2.2.6 Issue Committee Resolutions voted upon by the majority of its members to formalize important decisions reached by the Oversight Committee for implementation and adoption by its members and the CIIs.

4.1.2.3 **Creation of Technical Working Groups.** The Oversight Committee may create technical working group/s as necessary to undertake specific functions delegated by the Committee (i.e., information security, audit, etc.).

4.1.2.4 **Risk Management and Audit.** The Oversight Committee shall oversee the implementation of a comprehensive Risk Management Program on Cybersecurity. This includes conducting risk assessments, identifying vulnerabilities, legal and regulatory compliance, and ensuring appropriate risk mitigation strategies are in place, in line with ISO 31000, NIST 800-30, and other relevant internationally and locally recognized standards. Likewise, they shall oversee the conduct of regular audits to ensure the CIIs' compliance with these directives and other related rules.

4.1.2.5 **Incident Response and Coordination:** The Oversight Committee shall coordinate the sector-wide response to cybersecurity incidents. It ensures that an effective incident response plan is developed and established, based on NIST SP 800-61 and other internationally and locally recognized standards, and facilitates cooperation among stakeholders during incidents.

4.1.2.5.1 In case of escalation of a cyber-related incident into a disaster, the Committee shall coordinate with TFER on disruptions/disaster response actions caused by cybersecurity incident/s as necessary pursuant to Section 7.3 of DOE DC No. DC2022-06-0028.

4.1.2.6 **Information Sharing and Collaboration.** The Oversight Committee shall promote information sharing and collaboration among energy sector stakeholders, including government agencies, private sector entities, and international partners with a secure online platform. This is critical for proactive threat detection and response, leveraging online platforms and initiatives as outlined in EO 58 (s. 2024) and other laws and regulations.

4.1.2.7 **Compliance and Accountability.** The Oversight Committee shall ensure the compliance of CIIs with legal and regulatory requirements and conduct regular audits and assessments to uphold RA 10173, DOE circulars, and other relevant laws and regulations. It shall hold stakeholders accountable for their cybersecurity, and other relevant laws and mandates. In support thereof, the Oversight Committee shall:

4.1.2.7.1 Implement mechanisms and policies for the Cybersecurity Seal/Certificate of Compliance;

4.1.2.7.2 Recommend fiscal and non-fiscal incentives that would encourage compliance of CIIs and other energy industry stakeholders and participants; and

4.1.2.7.3 Recommend to the DICT sectoral recognition and awards for CIIs from the energy agencies/companies that exemplify excellent cybersecurity interventions and best practices.

4.1.2.8 **Education and Training.** The Oversight Committee shall facilitate the development of cybersecurity training programs and public awareness campaigns. It ensures that concerned personnel at all levels are equipped with the necessary knowledge and skills to address cybersecurity challenges, specifically:

4.1.2.8.1 Develop a Cybersecurity Upskilling Roadmap for the Energy Sector in collaboration with the DICT, academic institutions, development partners, and private agencies to increase the cybersecurity workforce capacity and awareness in the energy sector; and

4.1.2.8.2 Coordinate with relevant institutions and agencies to secure the prescribed training for members of the Committee and CIIs.

4.1.2.9 **Conduct of Meetings.** The Oversight Committee shall hold quarterly regular meetings, and such other special meetings as may be necessary upon the request of the Chairperson or at least two (2) of its members.

4.1.2.10 The Oversight Committee shall perform other functions that may be necessary and incidental to attain the objectives of this Circular.

4.2 **Creation of the Energy Sector Computer Emergency Response Team (ES-CERT-PH).** In accordance with Section 1.6 of the NCSP 2023-2028, the Energy Sector Computer Emergency Response Team (ES-CERT-PH) is hereby created as a Sector coordinating CERT-PH (SCERT-PH) to coordinate and oversee the various CII CERT-PHs of the energy sector. Energy companies identified as CII shall establish their Organizational CERT-PH to promptly respond and mitigate cybersecurity incidents of the company. The ES-CERT-PH shall report and collaborate directly with the NCERT-PH of the DICT to coordinate the sharing of relevant risk information and perform countermeasures and responses on cybersecurity incidents and situations from domestic and transnational sources affecting the energy sector.

4.2.1 **Composition of the ES-CERT-PH.** The ES-CERT-PH shall be led by the DOE. The members of the ES-CERT-PH shall be composed of the energy sector government agencies and private companies identified as CIIs (***Annex B***). The ES-CERT-PH shall be composed of the following:

4.2.1.1 The Head, who is the Director of the DOE Information Technology and Management Services (ITMS).

4.2.1.2 The members are the authorized representatives from each agency with at least a Division Chief rank or its equivalent rank from the IT Department or a unit performing IT management functions.

4.2.2 **Functions, Roles, and Responsibilities of the Head of the ES-CERT-PH.** The Head of the ES-CERT-PH shall have the following responsibilities and functions:

4.2.2.1 Coordinate with the DICT/NCERT-PH and facilitate incident handling and response as may be necessary for severe and critical cyber incidents in the energy sector;

4.2.2.2 Report the severe and critical cybersecurity incidents to the Chairperson of the Oversight Committee and Technical Secretariat;

4.2.2.3 Develop a manual of operations such as but not limited to an Incident Response Manual, playbooks, and Reporting Mechanism, in coordination with DICT/NCERT-PH for guidance in implementing cybersecurity measures, incident response procedures, and related activities;

4.2.2.4 Coordinate with the NCERT-PH and other trusted Information Sharing and Analysis Center (ISAC) on the access and issuance of advisories of ES-CERT-PH members for cybersecurity monitoring and cyber threat intelligence to assist in the detection and prevention of cyber incidents;

4.2.2.5 Work within a strict chain of command with the two top-level CERT-PHs (NCERT-PH and the Defense-CERT-PH as necessary);

4.2.2.6 Establish a Cyber Security Operations Center (SOC) for the energy sector as deemed necessary; and

4.2.2.7 Perform such other functions that may be necessary and incidental to attain the objectives of this Circular.

4.2.3 **Functions, Roles, and Responsibilities of the Members of the ES-CERT-PH.** The members of ES-CERT-PH shall have the following responsibilities and functions:

4.2.3.1 **Incident Detection and Analysis**. Monitor IT and OT systems and networks for potential security breaches and promptly identify malicious activities, specifically:

4.2.3.1.1 Identify threats by monitoring assets and anomalous activities; and

4.2.3.1.2 Triage and classify cybersecurity incidents within the organization.

4.2.3.2 **Threat Intelligence**. Gather, analyze, and disseminate information about current and emerging cyber threats to enhance proactive defense measures.

4.2.3.3 **Incident Handling and Response.** Take immediate and coordinated actions to contain and mitigate the impact of cybersecurity incidents, specifically:

4.2.3.3.1 Handle and respond to cybersecurity incidents; and

4.2.3.3.2 Develop and manage the cybersecurity response life cycle within the organization.

4.2.3.4 **Incident Monitoring and Reporting.** For severe or critical cybersecurity incidents, report and coordinate the response with the NCERT-PH and the ES-CERT-PH within the prescribed time period by the DICT using the prescribed reporting template, and also comply with the other reportorial and information requirements; ***(Please see Annex C for the Incident Reporting Flow Chart)***

4.2.3.5 **Risk and Vulnerability Management.** Identify and address risks and vulnerabilities in the IT and OT systems to prevent exploitation by malicious actors;

4.2.3.6 **Evidence Gathering and Forensics Analysis.** Cooperate with authorities in the conduct of thorough investigations post-incident to determine the root cause, assess the extent of damage, and recommend remedial actions, specifically:

4.2.3.6.1 Conduct damage and impact assessments on the affected facilities resulting from the cybersecurity incident; and

4.2.3.6.2 Cooperate with the authorized government agencies during the forensic analysis, investigation, and prosecution of cybercrimes and other violations against RA 10175 or the "Cybercrime Prevention Act of 2012".

4.2.3.7 **Training and Awareness**. Educate various stakeholders and employees about cybersecurity best practices, raise awareness about potential threats, and promote a culture of security within the organization. Activities shall include but not be limited to:

4.2.3.7.1 Conduct of cybersecurity tabletop simulations, drills, and exercises within the organization; and

4.2.3.7.2 Promotion and training of the organization in adopting a cyber-safe culture.

4.2.4 **Priority access of members of the ES-CERT-PH to the Services of the National Security Operations Center (NSOC) and National Computer Emergency Response Team - Philippines (NCERT-PH).** The ES-CERT-PH, through the DOE, shall coordinate with the NSOC and NCERT-PH under DICT to access and avail of the following services:

4.2.4.1 Link with the facilities and systems of the NSOC for the reporting of incidents, detection, monitoring, and rapid response to security incidents, and provision of cyber threat intelligence;

4.2.4.2 Conduct of baseline assessment of government agencies' cybersecurity posture;

4.2.4.3 Avail of Vulnerability Assessment and Penetration Testing services for government agencies and Government-Owned or Controlled Corporations (GOCCs);

4.2.4.4 Provision of Cyber Threat Intelligence and Monitoring; and

4.2.4.5 Establishment of an Incident Response Management for the members of the ES-CERT-PH.

4.2.5 **Professionalization and Capacity Building.** The DOE, in consultation with the DICT, shall develop and implement a continuous training program to enhance the skills of the OC-ESCCR, TWG-IDCII, ES-CERT-PH, and Technical Secretariat members, while also working towards their professionalization.

The Chairperson of the OC-ESCCR shall ensure that the members of the OC-ESCCR, TWG-IDCII, ES-CERT-PH, Technical Secretariat, and other relevant personnel participate in training or capacity development programs. Identified personnel must complete the prescribed basic or fundamental training or programs within six (6) months of their designation. Advanced or specialized training or certifications are to be undertaken upon their availability.

4.3 **Creation of the Technical Working Group on the Identification of CIIs (TWG-IDCII).** Pursuant to Section 3.2 of NCSP 2023-2028, a TWG on the identification of CIIs in the energy sector is hereby created in order to assess using a risk-based approach to identify and recommend the potential list of CIIs.

4.3.1 **Composition of the TWG-IDCII.** The TWG-IDCII shall be headed by the DOE and composed of members from government agencies, DOE Attached Agencies, and relevant energy stakeholders and participants:

4.3.1.1 **DOE Attached Agencies**

4.3.1.1.1 NEA
4.3.1.1.2 NPC
4.3.1.1.3 TransCo

4.3.1.1.4 PSALM
4.3.1.1.5 PNOC and its Subsidiaries (PNOC Renewables Corporation and PNOC Exploration Corporation)

4.3.1.2 **Other Government Agencies/Entities**

4.3.1.2.1 ERC
4.3.1.2.2 DICT
4.3.1.2.3 NICA
4.3.1.2.4 NSC Secretariat

4.3.1.3 The OC-ESCCR shall deliberate and approve the relevant government agencies, and energy sector stakeholders and participants that shall form part of the TWG-IDCII.

4.3.2 **Qualifications of TWG-IDCII Members.** The appropriate qualifications for the membership/agency representatives of the TWG-IDCII given its critical role in national security shall be established by the OC-ESCCR. The assigned TWG members shall also undergo security clearances, as necessary.

4.3.3 **Functions, Roles, and Responsibilities of the TWG-IDCII.** The TWG-IDCII shall have the following functions, roles and responsibilities:

4.3.3.1 **Develop the "Implementing Guidelines for Identifying the CIIs of the Energy Sector" using a risk-based approach**. The Implementing Guidelines shall be submitted for the approval of the OC-ESCCR. The guidelines shall include but not be limited to the following:

4.3.3.1.1 Defined criteria to be adopted by the energy sector based on the NCSP 2023-2028 and other relevant issuances. The criteria for the energy sector shall be endorsed to the Oversight Committee for approval and recommendation to the NCIAC; ***(Please see Annex C)***

4.3.3.1.2 Process flow, documentary/ reportorial requirements, information security protocols, and the timeline for the issuance of Certification of an Identified CII by the NCIAC; and

4.3.3.1.3 Audit, assessment procedures, and tools for the identification of the CII's Critical Information Technology Assets in Section 5.

4.3.3.2 **Submit the list of potential CIIs to the OC-ESCCR**, which shall then be endorsed to the DICT for evaluation. The DICT shall compile the recommendations and submit the same to the NCIAC, which will convene to discuss and recommend the

approval of the CII. Ultimately, the list of CIIs will be approved by the President of the Philippines;

4.3.3.3 Recommend to the OC-ESCCR the removal of CII designation as necessary;

4.3.3.4 Develop and submit to the OC-ESCCR the Audit Guidelines for Approved CIIs in the Energy Sector; and

4.3.3.5 Perform/deliver tasks to be delegated by the OC-ESCCR.

4.4 **Creation of a Technical Secretariat to the OC-ESCCR, the ES-CERT-PH, and TWGs.** The OC-ESCCR, ES-CERT-PH, and TWGs shall be provided technical and administrative support by the Energy Policy and Planning Bureau (Task Force on Energy Resiliency Secretariat) and other concerned units of the DOE to perform the following functions:

4.4.1.1 Provide Secretariat functions and technical support to the Oversight Committee to include development of the Rules of Procedure, plans and programs, guidelines, policy research and formulation, and coordination activities of members, among others;

4.4.1.2 Provide Secretariat functions and technical support to the ES-CERT-PH on the development of a manual of operations, playbooks, and incident response mechanisms, among others, in support of incident and cybersecurity risk management;

4.4.1.3 Provide Secretariat functions and technical support to the TWGs under the Oversight Committee;

4.4.1.4 Monitor the status of the implementation of this policy and Resolutions to be issued by the Oversight Committee;

4.4.1.5 Manage the submission of reports (i.e. Incident Reports, Assessment Reports, Audit Reports, etc.) from the CIIs, Audit Team, and other members;

4.4.1.6 Prepare reports, such as but not limited to progress reports, and accomplishment reports, for submission to the DOE Secretary and Chairperson of the OC-ESCCR;

4.4.1.7 Maintain a secure database of the training obtained by the cybersecurity professional workforce of the Committee members; and

4.4.1.8 Perform other tasks and functions delegated by the Chairperson.

4.5 **Identified Potential CIIs in the Energy Sector.** All concerned energy stakeholders or participants, once identified as **potential CII** based on the criteria, shall cooperate and comply with the requirements outlined in the implementing guidelines, including submission of relevant information and full participation in the assessments and validation activities of the TWG-IDCII.

4.6 **Approved CIIs in the Energy Sector.** Once approved by the President, all the CIIs in the energy sector shall undergo an onboarding process within 24 months based on the prescribed requirements by the DICT pursuant to Section 3.1.3 of NCSP 2023-2028 and other laws and regulations. The CII may also be given assistance on the following:

4.6.1 Qualification of securing its facilities from security threats with the aid of state forces such as the PNP and the AFP;

4.6.2 Use of Government Cybersecurity trust anchors when applicable; and

4.6.3 Annually, the DICT shall coordinate cybersecurity drills, trainings, and exercises with CII regulatory agencies, including some of their CII. The DICT shall also prioritize the cybersecurity training by NCERT-PH personnel for CIIs.

SECTION 5: CYBERSECURITY AND CYBER RESILIENCE POLICY FRAMEWORK

5.1 **Mandatory Compliances of CIIs to Cybersecurity Risk Reduction Regulations and Cyber Resilience Requirements.** The following requirements shall be complied with and submitted by the identified and designated CIIs in the energy sector to the DOE, ERC, and/or DICT:

5.1.1 Annual submission due on/before the **30th of April** to the DOE, ERC, and DICT of the **Cybersecurity Assessment Framework (CAF) Results**. The CAF is a standards-based framework that provides an evaluation methodology to determine the cybersecurity postures of both IT and OT applications and systems of energy infrastructure, as well as identify both the current state and a desired future state concerning the organization's risk management practices.

5.1.2 Annual submission due on/before the **30th of April** to the DOE, ERC, and DICT of the **Cyber Resilience Scorecard (CRS)**. The CRS builds on the CAF which develops a methodology considering cyber resilience at an organizational level and aligns with its cybersecurity outcomes. The CRS is incorporated as one of the pillars of the Energy Resilience Scorecard (ERS) pursuant to DOE DC No. DC2022-06-0028.

5.1.3 The CAF and CRS results shall be validated by an external auditor approved by the DICT. These shall serve as the required **Audit Report** to be submitted to the DICT based on the NCSP 2023-2028, in the absence of an external audit report from a private/independent third-party cybersecurity auditor.

5.1.4 Periodic submission of **Vulnerability Assessment and Penetration Testing (VAPT) Report** of identified Critical Information Technology Assets (i.e. IIoT, IoT) to the DICT.

5.1.5 **Quarterly Report** of cyber issues handled, closed, and remediated to be submitted to DICT, due **every last Monday of every Quarter**. Cyber

issues encompass various scenarios, including non-critical events, minor incidents, and attempted breaches. These efforts aim to oversee and gather intelligence on potential cyber threats or attacks that could escalate into larger-scale incidents.

5.1.6 **Cybersecurity and Cyber Resilience Program** to be submitted to DOE and ERC. This shall be developed based on the various assessment tools (i.e. Section 5.1.1 and 5.1.2) and shall be reviewed and updated every three (3) years thereafter from the first submission.

5.1.7 Compliance with all the assessments and reporting requirements shall be governed by the Data Privacy Act of 2012, and other relevant cybersecurity and cybercrime laws, rules, and regulations.

5.1.8 A secured online platform shall be developed by the Technical Secretariat to manage the submissions from the CIIs of the energy sector.

5.2 **Compliance Monitoring and Recognition for Best Practices.**

5.2.1 The OC-ESCCR, through the Technical Secretariat, shall monitor the submissions and compliances of the CIIs.

5.2.2 Energy industry stakeholders and participants who are highly compliant with the requirements of this policy and exhibit exemplary performance shall be endorsed by the OC-ESCCR to the DICT for recognition and awards.

5.2.3 Energy sector CIIs with basic compliances shall be provided guidance and intervention by the OC-ESCCR to achieve and improve regulatory compliances.

5.3 **Information Sharing and Mandatory Disclosure of Severe and Critical Cybersecurity Incidents.**

5.3.1 Any data provided, received, used, or otherwise obtained in connection with any matter relating to this Circular and other pertinent guidelines, shall be governed by the Data Privacy Act of 2012, confidentiality and intellectual property rules, and other relevant cybersecurity and cybercrime laws, rules, and regulations.

5.3.2 Information sharing among the OC-ESCCR, TWG-IDCII, ES-CERT-PH, NCIAC, NCERT-PH, National Cybersecurity Intelligence Network (NCIN), CICC, and other relevant stakeholders shall be guided by protocols (i.e. Traffic Light Protocol) and mechanisms based on the "National Security-and-Privacy-by-Design Framework" to be developed and prescribed by the DICT as well as ERC's rules on the treatment of confidential information. This includes the establishment of a Trusted Information Sharing Network (TISN).

5.3.3 Reports on cybersecurity incidents from the energy industry stakeholders and participants are classified information. However, incidents that potentially compromise the confidentiality, secrecy, and integrity of

Personal Information should be disclosed to the National Privacy Commission (NPC). The OC-ESCCR and ES-CERT-PH should, in compliance with the Data Privacy Act of 2012, inform data subjects within 72 hours that their Personal Information may have been exposed to allow risk mitigation.

5.4 **Adoption of Acceptable Cybersecurity Minimum Standards for Energy Sector CIIs.**

5.4.1 Government agencies from the energy sector classified and designated as CII shall be provided proper guidance by the OC-ESCCR in coordination with the DICT to allow each to adopt appropriate control measures relative to their capacity and budget.

5.4.2 CIIs from the energy sector stakeholders and participants shall adopt the acceptable and prescribed cybersecurity minimum standards approved by the OC-ESCCR.

5.5 **Accredited External Auditors, Third-Party Service Providers, and ICT Suppliers.** Pursuant to Section 3.1.2 of the NCSP 2023 - 2028, the energy industry stakeholders and participants shall utilize and consult with the recognized/accredited external auditors, third-party service providers, and ICT suppliers of the DICT.

5.5.1 Should the DICT initiate accreditation for external auditors, the relevant energy sector agencies shall adhere and comply therein and utilize the accredited external auditors.

5.5.2 The conduct of the audit shall be based on the guidelines recommended by the TWG-IDCII and approved by the OC-ESCCR.

5.5.3 The ES-CERT-PH shall provide a whitelist of recommended third-party service providers and ICT suppliers to the DICT, which will undergo risk assessment, evaluation, and required security measures. The third-party service providers and ICT suppliers must adhere to the prescribed cybersecurity minimum standards, the Data Privacy Act of 2012, and other policies and security measures.

5.5.4 The energy sector CIIs shall only consult with DICT-accredited and recognized VAPT service providers.

5.6 **Development of the Cybersecurity Professionals and Expertise in the Energy Sector.** In order to achieve Outcome 2 under the NCSP 2023-2028, the energy sector enjoins in the implementation of the cybersecurity workforce strategy in order to attain the required number of cybersecurity professionals in both the private and public sectors through the following:

5.6.1 A Cybersecurity Upskilling Roadmap for the Energy Sector shall be developed in partnership with the DICT, which shall include ladderized training and its qualification requirements on cybersecurity targeting the

members of the OC-ESCCR, ES-CERT-PH, TWGs, and other concerned entities/individuals.

5.6.2 The members of the OC-ESCCR, ES-CERT-PH, and TWG-IDCII are highly encouraged to have 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 Manager (CISM).

5.6.3 Energy industry stakeholders and participants are highly encouraged to undergo cybersecurity certifications, attend various training programs and activities geared towards up-skilling and re-skilling the workforce, and utilize widely accepted frameworks such as the ISO and NIST Risk Management Framework, among others. The private sector or academic institutions may also be tapped to provide training on cybersecurity.

5.6.4 Government personnel who acquire government-sponsored and private-sector cybersecurity training must undergo a Return of Service and fulfill the service obligations based on the existing Civil Service Commission (CSC) guidelines. The private sector agencies are likewise encouraged to adopt policies that would build and achieve retention of the cybersecurity professional workforce in the energy sector.

5.6.5 The Technical Secretariat shall maintain a database of the trainings obtained by the cybersecurity professional workforce for monitoring purposes.

SECTION 6: MANPOWER COMPLEMENT AND FUND SUPPORT

6.1 The DOE, as the lead agency of the various organizations created for this Circular, shall undergo institutional strengthening through the establishment of dedicated units and/or personnel to ensure the proper implementation of this Circular.

6.1.1 The DOE shall coordinate with the DICT and DBM in the development of a cybersecurity division/units and its appropriate manpower complement. Pending the provision of *plantilla* positions in government, the DOE is hereby authorized to augment or recommend the hiring of additional personnel as deemed necessary to ensure the seamless implementation of this Circular.

6.1.2 The private sector organizations, especially the CIIs, are encouraged to create dedicated positions to fulfill the requirements of this Circular.

6.2 The funds to support this Circular, include the budgetary requirements necessary to cover the personnel services, procurement of supplies/equipment, maintenance and other operating expenditures, and capital outlay for the implementation of the Cybersecurity and Cyber Resilience plans, programs, and activities, shall be sourced from the General Appropriations Act (GAA) subject to the usual planning, budgeting and accounting rules and regulations. Thereafter, the DOE shall ensure that activities are programmed in its annual appropriations.

6.3 All of the DOE, including personnel providing technical support to the implementation of the Cybersecurity program, services, and projects, shall be entitled to the benefits outlined in RA 8439, as amended by RA 11312, known as the Magna Carta for Scientists, Engineers, Researchers, and other Science and Technology Personnel in Government Service.

6.4 Private companies are highly encouraged to allocate funds for the implementation of their Cybersecurity and Cyber Resilience plans and programs.

6.5 DOE Attached Agencies and the ERC shall allocate funds for Cybersecurity and Cyber Resilience plans and programs in their annual budget proposal subject to the existing guidelines of the DBM.

6.6 DOE Attached Agencies and the ERC may coordinate with the DICT, DBM, or other appropriate government agencies in the development of a cybersecurity division/unit and its appropriate manpower complement.

SECTION 7: REVIEW AND CONTINUAL IMPROVEMENT

7.1 The OC-ESCRR shall review and evaluate the effectiveness of the *Energy Sector Cybersecurity and Cyber Resilience Policy* and its programs every three (3) years, or when deemed necessary.

7.2 Energy industry stakeholders and participants shall include under the Cyber Resilience Pillar their Cybersecurity plans and programs and their updates in the Resiliency Compliance Plan (RCP) submissions required in the DOE DC Nos. DC2018-01-0001 and DC2022-06-0028.

SECTION 8: PENAL PROVISION

8.1 This Circular shall adopt the applicable penal provisions as provided in RA 11659, otherwise known as the Amended Public Service Act, its Implementing Rules and Regulations, and other relevant laws and regulations.

SECTION 9: REGULATORY SUPPORT

9.1 The DOE, within six (6) months from the effectivity of this Circular, shall convene the organization and coordinate with other concerned government agencies and energy industry stakeholders and participants, for the issuance of the appropriate guidelines and policies for the implementation of this Circular.

9.2 The ERC shall provide and develop appropriate regulatory support to the CIIs from the energy stakeholders upon the promulgation of this Circular, which includes but is not limited to incentives, cybersecurity performance metrics, and cost recovery mechanisms for cybersecurity-related investments.

9.3 In the case of regulated entities, such as transmission companies, distribution utilities, and others, the recovery of capital expenditures, operation and maintenance expenses, and other related expenses that impact electricity rates are subject to the evaluation and approval of the ERC.

SECTION 10: SEPARABILITY CLAUSE

If for any reason, any section or provision of this Circular is declared unconstitutional or invalid, the other parts or provisions hereof that are not affected thereby shall continue to be in full force and effect.

SECTION 11: REPEALING CLAUSE

Nothing in this Circular shall be construed as to amend, supersede, or repeal any of the mechanisms or institutions already existing or responsibilities already imposed and provided for under any existing law, rule, or contract.

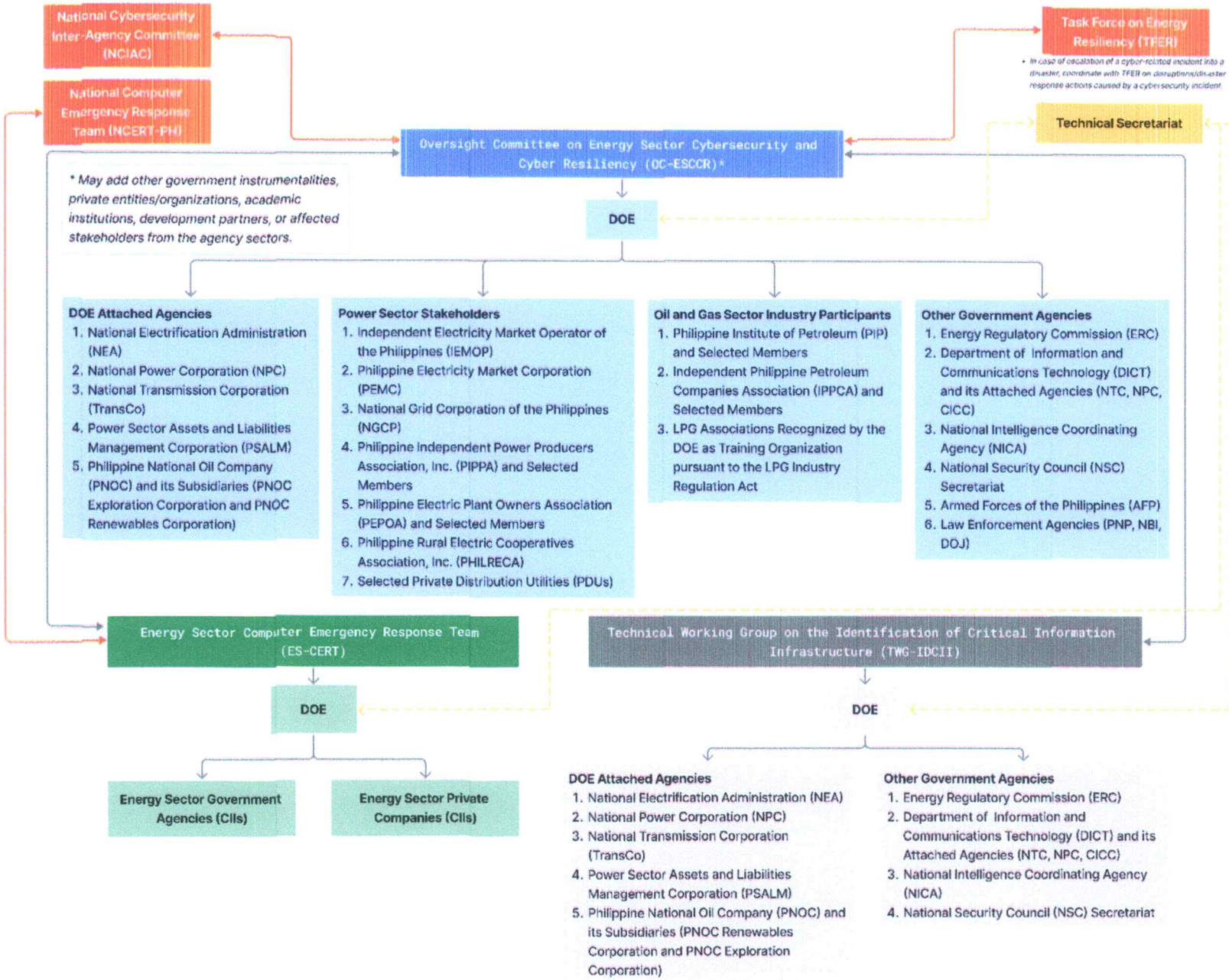
SECTION 12: EFFECTIVITY

This Circular shall take effect fifteen (15) days after its publication in at least two (2) newspapers of general circulation. A copy of this Circular shall be filed with the University of the Philippines Law Center - Office of National Administrative Register.

Issued on JAN 23 2025 at the DOE, Energy Center, Rizal Drive cor. 34th St., Bonifacio Global City, Taguig City.

RAPHAEL P.M. LOTILLA
Secretary

Annex A: Organizational Structure



Annex B: Criteria for Identifying CIIs

The TWG-IDCII shall review and recommend the appropriate Criteria for Identifying CIIs prescribed in the NCSP 2023 - 2028 to the Oversight Committee. This shall include, but not be 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 in 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 of facilities may lead to disastrous environmental effects (e.g. unauthorized release of water from dams, release of untreated water, and nuclear meltdown)

Annex C: Incident Reporting Flow Chart