CONGRESS OF THE PHILIPPINES
TWENTIETH CONGRESS
First Regular Session

HOUSE OF REPRESENTATIVES

H. No. 9461

BY REPRESENTATIVES VALERIANO, SUANSING (B.V.), PUNO, VELOSO-TUAZON, LAGBAS, TOLENTINO, ORETA, ACOP, SUANSING (M.A.), YAP (ERIC), ISMULA, DIOKNO, CENDAÑA, BAG-AO, SUAN, SOLON, MONTES, PLEYTO, ROMAN, OAMINAL (H.), CO, ELAGO, CHUA-TAI, EMANO, ODUCADO, LABADLABAD, CHAN (J.F.N.J.), LACSON, BAUTISTA (J.M.), TAN (K.M.), DY (F.), MARCOS, CARI, GONZALES (A.M.), ARENAS, DE LIMA, SAKALURAN, ESCUDERO, DIMAGUILA, CUA, FLORES, VERGARA, ATAYDE, MATIBAG, BERNOS (J.), PIMENTEL, FUENTEBELLA, RODRIGUEZ (R.), ORDANES, POE, AQUINO-MAGSAYSAY, BAUTISTA-LIM, ESPARES, GALANG, REGENCIA, ADIONG, ZAMORA (Y.M.), CHUA AND CO-PILAR

AN ACT
STRENGTHENING CHILD PROTECTION SAFEGUARDS, REGULATORY MEASURES, POLICIES AND ENFORCEMENT MECHANISMS AGAINST ONLINE SEXUAL ABUSE OR EXPLOITATION OF CHILDREN (OSAEC) AND CHILD SEXUAL ABUSE OR EXPLOITATION MATERIALS (CSAEM), REPEALING FOR THE PURPOSE REPUBLIC ACT NO. 11930, OTHERWISE KNOWN AS THE "ANTI-ONLINE SEXUAL ABUSE OR EXPLOITATION OF CHILDREN (OSAEC) AND ANTI-CHILD SEXUAL ABUSE OR EXPLOITATION MATERIALS (CSAEM) ACT," PROVIDING PENALTIES FOR VIOLATIONS THEREOF AND APPROPRIATING FUNDS THEREFOR

Be it enacted by the Senate and House of Representatives of the Philippines in Congress assembled:

CHAPTER I
PRELIMINARY PROVISIONS

SECTION 1. ***Short Title.*** – This Act shall be known as the "Child Online Safety and Protection Act of 2026."

SEC. 2. ***Declaration of Policy.*** – The State recognizes the vital role of children and youth in nation-building and shall promote and protect their dignity, safety, development, and physical, moral, spiritual, intellectual, emotional, psychological, and social well-being.

Consistent with this policy, the State shall provide special protection to every child from all forms of sexual violence, abuse, and exploitation, whether committed online, offline, or through a combination of both, by strengthening measures for prevention, deterrence, and intervention against Online Sexual Abuse or Exploitation

of Children (OSAEC) and Child Sexual Abuse or Exploitation Materials (CSAEM) and related forms of technology-facilitated child sexual abuse or exploitation, while ensuring that child victims and survivors are protected, supported in their recovery and reintegration, and given meaningful access to justice.

To this end, the State shall:

(a) Guarantee the fundamental rights of every child from all forms of neglect, cruelty and other conditions prejudicial to development;

(b) Protect every child from all forms of sexual abuse or exploitation, whether committed online, offline, or through a combination of both, including the creation, production, distribution, facilitation, or monetization of exploitative performances or materials, and the inducement, coercion, recruitment, grooming, persuasion, or facilitation of a child to engage in, participate in, assist, or be involved in any form of OSAEC and CSAEM or related child sexual abuse or exploitation;

(c) Comply and align with international treaties concerning the rights of a child to which the Philippines is a State party or may hereafter become a party, which include, but is not limited to, the United Nations (UN) Convention on the Rights of the Child, the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, the International Labour Organization (ILO) Convention No. 182 on the Elimination of the Worst Forms of Child Labour, and the Convention against Transnational Organized Crime, and take guidance from other relevant international instruments consistent with the Constitution and existing laws;

(d) Comply and align with international treaties and conventions concerning cybercrime, transnational crime, and digital evidence, to which the Philippines ~~is~~ a State Party or may hereafter become a party, including the Convention on Cybercrime (Budapest Convention) and their applicable protocols, and take guidance from other relevant international instruments consistent with the Constitution and existing laws, recognizing that OSAEC is primarily a cybercrime that transcends borders and necessitates timely and lawful cross-border cooperation and sharing of information;

(e) Ensure the right of children to useful, meaningful and safe access to digital technologies that will provide knowledge and develop their understanding of civil, political, cultural, economic and social rights and help them achieve their potential to be empowered, responsible, law-abiding citizens, with the end in view of protecting them from any form of violence online and offline;

(f) Provide paramount consideration to the interests of children in all actions affecting them, whether undertaken by public or private social welfare institutions, courts of law, executive agencies, law enforcement agencies, local government units (LGUs), legislative bodies, and private business enterprises especially those related to the online safety and protection of children;

(g) Recognize that OSAEC and CSAEM are not only violations of children's rights but also constitute a serious threat to national security, social cohesion, and public health, given their long-term psychological, emotional, and socio-economic impact on children, families, and communities, and the transnational, organized, and recurring nature of these offenses;

(h) Ensure that internet intermediaries, device manufacturers, technology platforms, payment service providers, learning institutions, and other covered entities exercise a heightened duty of care towards children by adopting child-protection standards, safety-by-design principles, age-appropriate safeguards, and prompt measures to prevent, detect, report, and disrupt OSAEC and CSAEM, while enabling children's safe, meaningful, and productive use of digital technologies;

(i) Institutionalize a whole-of-government and whole-of-society response through a permanent national coordination mechanism against OSAEC and CSAEM, ensuring clear roles, effective information-sharing, joint operations, and data informed policymaking among national government agencies, local government units, law enforcement, prosecution offices, regulators, civil society, the private sector, and international partners; and

(j) Recognize the importance of safe, meaningful, and survivor-informed participation in the formulation, implementation, monitoring, and evaluation of laws, policies, programs, and measures under this Act. Survivor participation shall be voluntary, trauma-informed, child-sensitive, survivor-centered, and subject to appropriate safeguards for confidentiality, safety, well-being, and the best interests of the child.

SEC. 3. ***Definition of Terms.*** – As used in this Act:

(a) ***Child*** refers to a person below eighteen (18) years of age, or those eighteen (18) years of age or over, but are unable to fully take care of themselves or protect themselves from abuse, neglect, cruelty, exploitation, or discrimination because of physical, mental, intellectual, or sensory disability or condition.

For purposes of determining whether a material, depiction, representation, advertisement, offer, solicitation, transaction, livestream, performance, or similar subject matter involves a child under this Act, the term "child" shall also refer to:

(1) A person regardless of age, who is presented, advertised, offered, represented, depicted, or portrayed as a child; and

(2) Any image, representation, graphic, visual depiction, drawing, illustration, painting, sketch, animation, or similar material that depicts, purports to depict, or is made to appear to be a child, whether manually created or generated, altered, manipulated, or synthesized in whole or in part through the use of digital, electronic, mechanical, computational, or other technological means, including artificial intelligence, machine learning systems, software, synthetic media, and content commonly referred to as "deepfake," regardless of whether any real child was involved in its creation.

Paragraphs (1) and (2) shall not apply to provisions that, by their nature, require an actual child victim, actor, or participant, including provisions on recruitment, transport, harboring, receipt, hiring, use, inducement, coercion, participation, assistance, rescue, protection, non-liability, exemption from liability, victim services, recovery, reintegration, or aftercare, unless otherwise expressly provided in this Act.

(b) ***Child sexual abuse*** refers to any act, whether committed through communication by any means or platform, or through physical contact or interaction, by which a child is used, induced, enticed, coerced, manipulated, or caused to participate in or undergo any act for the sexual stimulation or gratification of any person, or for the purpose of pursuing or engaging in sexual activity or having carnal knowledge with the child, regardless of the gender of the offender or the child, and regardless of the child's purported consent.

(c) ***Child sexual abuse or exploitation material (CSAEM)*** refers to any representation, whether offline, or by, through, or with the use of technology or of information and communications technology (ICT), by means of visual, video, audio, written, data, or any combination thereof, by electronic, mechanical, digital, optical, magnetic or any other means, of a child engaged or involved in real or simulated sexual activity as defined in this Act; or that depicting acts of sexual abuse or exploitation of a child; or that focuses on the genitalia, anus, breasts or other body parts of a child or characteristics of a child for sexualization, whether or not nudity is complete.

For clarity, an image, representation or graphic, digitally or manually created, through the use of software, artificial intelligence, any type of machine learning system, or any similar ICT tool, in whole or in part, which depicts any act of child sexual abuse, child sexual exploitation, or sexual activity involving a child, shall be considered CSAEM, whether or not it is based on the image, likeness, or data of an actual child.

CSAEM Synthetic Media under Section 3(k) of this Act shall also be considered CSAEM.

(d) ***Child sexual exploitation*** refers to any act by which a child is sexually abused, used, induced, enticed, coerced, manipulated, or subjected to sexual activity for the benefit, advantage, gratification, profit, gain, favor, consideration, or other exploitative purpose of the offender or any other person, whether monetary or non-monetary, and regardless of the child's purported consent. It includes:

(1) The commission of child sexual abuse in exchange for, or in expectation of, money, profit, consideration, favor, benefit, advantage, or any other thing of value, whether received by the offender, the child, or any other person;

(2) The use of a child in actual or simulated sexual activity, or in any act of a sexual nature, for the gratification, benefit, advantage, or profit of another person;

(3) The employment of fraud, machination, undue influence, intimidation, threat, coercion, manipulation, deception, abuse of authority, or abuse of vulnerability to cause, induce, maintain, or facilitate the sexual abuse of a child, sexual activity with a child, or the use of a child for any exploitative sexual purpose; and

(4) Any other similar or analogous act by which a child is sexually abused or exploited for the gratification, benefit, advantage, or profit of another person.

(e) ***Competent authority*** refers to law enforcement agencies, government entities vested with authority to investigate offenses, government entities with prosecutorial functions, courts, regulators, or the National Child-Safety Command and Operations Service (NC-COpS).

(f) ***Computer*** refers to an electronic, magnetic, optical, electrochemical, or other data processing or communications device, or grouping of such devices, capable of performing logical, arithmetic, routing, storage, or communication

functions and which includes any storage, communications, input, output, or other facility or equipment directly related to or operating in conjunction with such device or group of devices. It covers, but is not limited to, any type of computer device including devices with data processing capabilities or communications capabilities like mobile phones, smartphones, tablets, servers, computer networks and other devices, whether or not connected to a network or the internet.

(g) ***Computer data*** refers to any representation of facts, information, concepts, signs, signals, writings, images, sounds, or instructions in a form suitable for processing in a computer system, including a suitable program that can enable a computer system to perform a function, and includes electronic documents, data messages, and other data, whether stored locally, remotely, or online.

For purposes of this Act, subscriber information, traffic data, and content data are specific categories of computer data, as separately defined under this section.

(h) ***Content data*** refers to the content of the communication, the meaning or purport of the communication, or the message or information being conveyed by the communication, other than traffic data, or subscriber's information/registration information.

(i) ***Covered Entities*** refer to internet intermediaries, internet service providers (ISPs), technology platforms, payment service providers (PSPs), virtual asset service providers (VASPs), public wifi, internet hotspots, cafes or kiosks, learning institutions, supplementary learning and youth activity centers, whether public or private, including those owned, operated or controlled by the government, government-owned or -controlled corporations, and other public or private entities with duties and responsibilities defined under this Act.

(j) ***Covered Entities with Enhanced Safeguarding Duties*** refer to covered entities designated by the National Council for Child Online Safety and Protection (NCC), upon recommendation of the NC-COpS and in consultation with the appropriate sectoral regulators or competent authorities, as requiring enhanced safeguards against OSAEC, CSAEM, or related technology-facilitated child sexual abuse or exploitation, by reason of scale, user reach, transaction volume, functionality, systemic impact, technical architecture, or repeated identification in official or recognized reports under this Act.

(k) ***CSAEM Synthetic Media*** refers to any text, audio, image, representation, graphic, visual depiction, video, or any combination thereof, whether generated, altered, manipulated, or synthesized in whole or in part through

digital, electronic, mechanical, computational, or other technological means, including artificial intelligence, machine learning systems, software, or similar tools, which depicts, represents, or appears to depict a child as nude, engaged in sexual activity, or subjected to sexual abuse or sexual exploitation, whether or not based on the image, likeness, voice, data, or other identifying attributes of an actual child, and whether involving wholly synthetic persons, real persons, or any combination thereof.

(l) ***Data Transmission Industry Participant (DTIP)*** refers to any entity engaged in the provision of data transmission services as a form of economic activity. Public telecommunications entities (PTEs) and VASPs, as defined under Republic Act No. 7925 or the "Public Telecommunications Policy Act of the Philippines," and Satellite Systems Providers or Operators (SSPOs) are considered DTIPs to the extent of their businesses engaged in data transmission services, excluding foreign government-controlled entities or state-owned enterprises, except independent pension funds, sovereign wealth funds, and multinational banks.

For the purposes of this Act, the term DTIP and VASP shall be used interchangeably.

(m) ***Device manufacturer*** refers to any natural or juridical person that designs, develops, assembles, imports or distributes electronic devices primarily intended for the capture, creation, storage, processing, or transmission of digital images, videos, audio recordings, or electronic communications, which may reasonably be used to produce, facilitate, or distribute CSAEM.

This includes, but is not limited to, mobile phones, computers, tablets, digital cameras, webcams, and other communication or media-capable devices designed for content creation, storage, or digital communication.

For the avoidance of doubt, the term does not include manufacturers, importers, or distributors of:

(1) Devices in which imaging, storage, or connectivity functions are merely incidental to the device's primary purpose and which are not ordinarily used for the creation, storage, or transmission of visual, audio, or electronic communications, such as household appliances, industrial equipment, or similar connected devices; and

(2) Individual components, parts, subassemblies, or embedded elements of such devices, such as semiconductors, microchips, motherboards, sensors, memory modules, or similar parts, unless such components

are themselves marketed or distributed as standalone media-capable or communication-capable devices.

(n) ***First-person produced CSAEM*** refers to any CSAEM that is created, captured, recorded, generated, transmitted, or otherwise produced by a child as defined in the first paragraph of Section 3(a), where such child is the sole actual child depicted, portrayed, or represented in the material.

For the avoidance of doubt, the term applies only where the child creator and the child depicted are one and the same actual child, and no other actual child is depicted, portrayed, or represented in the material.

(o) ***Grooming*** refers to any deliberate act, repeated act, series of acts, or any form of communication, whether done in person or through ICT, directed at a child or someone who is believed to be a child, or the child's parent, guardian, or caregiver, and intended to build trust, gain access, exert influence, or establish control over the child and/or such parent, guardian, or caregiver for any of the following purposes, whether or not such purpose is explicitly stated in the acts or communications:

(1) Perpetrating or facilitating any sexual activity;
(2) Producing, creating, disseminating, or transmitting any form of CSAEM;
(3) Normalizing sexual conversations, conduct, or content involving or directed at the child; or
(4) Arranging, attempting to arrange, or facilitating in-person or real-time contact, meetings, or encounters with the child, where, having regard to the acts or communications and the circumstances in which they occur, there is reasonable cause to believe that such contact is intended for any of the foregoing purposes.

For purposes of this Act, grooming is deemed committed upon the performance of any such act, even if none of the foregoing purposes is achieved, no sexual activity occurs, and no subsequent abuse or exploitation takes place.

This definition shall not include acts or communications between two minors where the age difference between them is not more than three (3) years: *Provided,* That the act or communication in question is shown to be non-coercive, non-abusive, and non-exploitative.

(p) ***Information and Communications Technology (ICT)*** refers to the totality of electronic means to access, create, collect, store, process, receive, transmit, present and disseminate information.

(q) ***Internet address*** refers to the uniform resource locator or internet protocol address of an internet site.

(r) ***Internet asset*** refers to any identifiable digital resource that is accessible on or through the internet or an internet-connected network, including, but not limited to, an Internet site, domain name, uniform resource locator (URL), internet protocol (IP) address or range, server, account, application, page, profile, channel, group, listing, storage location, or device or node participating in a peer-to-peer or other distributed network.

For purposes of this Act, the term covers any such internet asset that is used, or reasonably suspected of being used, to commit, facilitate, or transmit violations of this Act.

(s) ***Internet café or kiosk*** refers to an establishment or any place or venue that offers or proposes to offer the use of its computer/s or computer system for the purpose of accessing the internet, computer games or related activities: *Provided,* That for the purposes of this Act, non-formal business establishments that provide internet services shall also be considered as internet café or kiosk.

(t) ***Internet hotspot*** refers to an establishment or any place or venue that offers access to the internet. It includes hotels or motels, malls, restaurants, internet cafes or kiosks, public spaces or other related/similar places;

(u) ***Internet intermediaries*** refer to any natural or juridical person that provides infrastructure or services which enable users to access, transmit, route, cache, host, store, share, disseminate, index, search for, or otherwise make available third-party content, products, services, or applications on or through the Internet.

The term includes, among others:

(1) Internet service providers (ISPs) and other internet access providers;
(2) Virtual private network services (VPNs);
(3) Web hosting providers, including domain name registrars, cloud storage and file-sharing services, and content-delivery network (CDN) services;
(4) Internet search engines and web portals;
(5) E-commerce intermediaries, including online marketplaces and platforms that facilitate the offer, listing, or sale of third-party goods or services;
(6) Virtual asset service providers;
(7) Participative network platform providers, including social media and other content-sharing platforms, video-sharing services, online forums, rating or review platforms, messaging or community services that support

user-generated content, and online games or virtual worlds with user-generated content or communications between users;

(8) Application stores and digital application marketplaces through which users access or obtain Internet-connected applications or services; and

(9) Other entities performing materially similar functions.

"Internet intermediary" covers any natural or juridical person that designs, develops, operates, controls, provides, or makes such services or facilities available in or into the Philippines, whether or not it has a physical presence in the country.

(v) ***Internet service provider (ISP)*** refers to a public telecommunication entity (PTE) or data transmission industry participant that provides users or other entities with data connection allowing access to the Internet through physical transport infrastructure, and such access is necessary for internet users to access content and services on the internet, and for content providers to publish or distribute materials online.

(w) ***Internet site*** refers to a website, bulletin board service, internet chat room, newsgroup, or any other Internet or shared network protocol address.

(x) ***Luring*** refers to the act of knowingly and intentionally communicating, by means of a computer system or any ICT, directly with a child or a person whom the offender believes to be a child, for the purpose of enticing, inducing, soliciting, inviting, or persuading the child to:

(1) Engage in any sexual activity, or submit to any act of sexual abuse or sexual exploitation;
(2) Participate in the production, creation, performance, transmission, or livestreaming of any form of CSAEM;
(3) Engage in sexual conversations, conduct, or content; or
(4) Meet in person, appear online in real time, or otherwise make himself/herself available for any act intended to result in the commission of the acts described in subparagraphs (1) or (2).

For purposes of this Act, luring is deemed committed upon the making of such communication with the foregoing purpose, whether or not the child responds, agrees, participates, meets the offender, or any sexual activity or CSAEM-related act is ultimately carried out.

This definition shall not include acts or communications between two minors where the age difference between them is not more than three (3)

years, provided that such acts or communications are shown to be non-coercive, non-abusive, and non-exploitative.

(y) ***Online Sexual Abuse or Exploitation of Children (OSAEC)*** refers to any conduct in which information and communications technologies are used as an instrument, venue, or means to sexually abuse and/or exploit a child. This can also include cases in which offline child sexual abuse and/or exploitation is combined with an ICT component.

This includes, but is not limited to, the use of ICT as an instrument, venue, or means to commit the following:

(1) Production, creation, procurement, solicitation, distribution, advertising, sale, offering, access, viewing, livestreaming, publication, promotion, or possession of CSAEM;
(2) Grooming and luring of a child as defined in this Act;
(3) Child sexual extortion as defined in this Act;
(4) Image-based sexual abuse of a child as defined in this section;
(5) Pandering as defined in this Act;
(6) Prostitution of a child; and
(7) Sexualization of a child.

Image-based Sexual Abuse of a Child (ISA) refers to a form of technology-facilitated sexual violence against a child, whether committed as a single act or as part of a pattern of conduct, that involves the recording, capturing, creation, use, sharing, transmission, publication, or distribution of, or threats to share, transmit, distribute, or publish, any nude or sexual text, audio, image, visual representation, or video of a child as defined in Section 3(a) of this Act.

ISA includes, but is not limited to, sexual extortion and the use of artificial intelligence, machine-learning systems, or other technologies to produce, construct, manipulate, synthesize, or otherwise generate CSAEM, including digitally manipulated, AI-generated, "deepfake" live-synthetic, or other similar technology-driven CSAEM, whether or not based on the image, likeness, or data of an actual child.

(z) ***Pandering*** refers to the act of offering, advertising, promoting, representing or distributing through any means any child sexual abuse or exploitation material, or any material that purports to contain any form of child sexual abuse or exploitation material, regardless of its actual content.

(aa) ***Participative network platform provider*** refers to any person or entity, including social media intermediary, that facilitates social communication and

information exchanges which are based on online technologies such as web, instant messaging, or mobile technologies, that enable users to contribute to developing, rating, collaborating, and distributing internet content and developing and customizing internet applications or to conduct social networking. It may also refer to a person or an entity that provides a platform or site for blogging, video-sharing, picture-sharing, file-sharing sites, online gaming, or instant messaging, among others.

(bb) ***Payment service provider (PSP)*** refers to any natural or juridical person that owns, operates, manages, or provides a payment system or payment service, which enables the transfer, exchange, acceptance, acquisition, processing, storage, or settlement of monetary value, in fiat currency, conducted electronically, online or in person, or through any other channel, and whether domestic or cross-border in nature.

The term includes, whether directly or through a technological platform:

(1) Banks, non-bank financial institutions (NBFIs);
(2) Electronic money issuers (EMIs), money service businesses, e-wallet operators, remittance and transfer agents;
(3) Merchant acquirers, payment gateways and processors, card issuers, card networks, and clearing or switch operators;
(4) Operators of payment systems (OPs), when performing payment or transfer functions; and
(5) Any other entity that, by the nature of its activities, performs equivalent payment, clearing, or settlement functions.

An entity that offers, markets, or makes such payment services available in or into the Philippines, whether or not it has a physical presence in the country, shall be deemed a PSP under this Act.

(cc) ***Person*** refers to any natural or juridical entity.

(dd) ***Prostitution*** refers to any act, transaction, scheme or design involving the use of a person by another, for sexual intercourse or lascivious conduct in exchange for money, profit, or any other consideration.

(ee) ***Regulator*** refers to any government agency, body, department, bureau, office, instrumentality, service, commission, or authority empowered by this Act or other relevant law to regulate, administer, or adjudicate matters affecting substantial rights and interests of private persons and entities covered by this Act.

(ff) ***Sexual activity*** includes the following acts, whether actually performed or simulated:

(1) Sexual intercourse or lascivious act, including contact involving the genitalia, oral stimulation of the genitals or oral stimulation of the anus, whether between persons of the same or opposite sex;
(2) Masturbation;
(3) Sadistic or masochistic abuse;
(4) Lascivious exhibition of the genitals, buttocks, breasts, pubic area and anus;
(5) Bestiality;
(6) Use of any object or instrument for lascivious acts; or
(7) Any other analogous circumstance.

(gg) ***Sexual or Sadistic Extortion*** of a child refers to any act whereby a person, through either deceit, grooming, manipulation, inducement, enticement, persuasion, solicitation, coercion, intimidation, threat to produce or disseminate any nude or sexual text, conversation, audio, image, visual representation, video, livestream, or other CSAEM, any form of threat, abuse of authority, misuse of images or personal data, or misuse of information and communications technologies, knowingly demands, obtains, or attempts to demand or obtain from a child or any member of the child's family, any of the following:

(1) Any CSAEM, including first person produced CSAEM by the child;
(2) Any material showing sadistic or masochistic abuse, whether directed at themselves or others or a live animal;
(3) The performance by the child of any sexual act or sexual activity, whether live, streamed, recorded, or in person;
(4) The perpetration by the child of any physical, psychological or sexual violence, harm, abuse, cruelty or exploitation, whether directed at themselves or others;
(5) Any monetary, proprietary, or other benefit; or
(6) Any other act of compliance demanded or imposed by the offender.

Sexual extortion likewise covers any act where the person from whom any CSAEM, sexual act, monetary or other benefit, or act of compliance is demanded is already of legal age at the time of the extortion, if in the case of a threat to produce or disseminate CSAEM, the CSAEM or material used or threatened to be used for such extortion was produced, created, or obtained when such person was a child as defined in Section 3(a) of this Act.

For purposes of this provision, "family" refers to the child's relatives by consanguinity or affinity up to the second degree.

(hh) ***Sexualization of a child*** refers to any act by which a person uses, portrays, represents, directs, or causes a child to be used or portrayed as a sexual object for the sexual desire or satisfaction of oneself or another, even if there is no physical contact, actual sexual intercourse, or display of nudity or private parts, and whether committed offline or through ICT.

This can also include:

(1) Posting, choreography, gestures, or conduct that depict or simulate sexual activity, suggestive touching, or sexualized dances;
(2) Staging, attire, props, or settings directed at or imposed on a child to create a sexualized context;
(3) Lascivious focus on a child's body or specific body parts (including buttocks, breasts, genital or pubic area), even without nudity, through camera angles, zoom, cropping, or narration intended to sexualize;
(4) Creation, capture, editing, curation, or dissemination of sexualized images of a child;
(5) Sexualized solicitation or commentary directed at a child;
(6) Digitally manipulated materials, including deepfakes, that portray a child, or a person made to appear to be a child, in a sexual manner; or
(7) The production, manufacture, creation, design, assembly, importation, sale, offer, distribution, advertisement, promotion, procurement, possession, or use of a child-like sex doll, mannequin, robot, device, or three-dimensional representation that depicts, is made to appear as, or is marketed as representing a child or child-like person, and is designed, adapted, or promoted for sexual use, sexual gratification, or simulation of sexual activity.

This definition does not include legitimate medical, educational, therapeutic, or law enforcement activities that are reasonably necessary, proportionate, and conducted in an appropriate and professional manner, and not undertaken for the sexual arousal, gratification, or sexualized entertainment of any person.

(ii) ***Solicit*** refers to any request, command, persuasion, inducement, enticement, encouragement, proposal, invitation, or advertisement, or offer of any consideration, whether monetary or non-monetary, made to another person, directly or indirectly, publicly or privately, in person or through any means of ICT, including technology platforms and software whether usable online or offline, to perform an act.

(jj) ***Streaming*** refers to the broadcasting, transmission, delivery, display, reception, or viewing of audio, visual, audiovisual, or similar content through the use of ICT, whether the recipient or viewer is passively watching or

listening, or actively communicates with, directs, requests, or otherwise influences the content. It is considered livestreaming when the broadcasting, transmission, delivery, display, reception, or viewing occurs in real time or substantially in real time.

(kk) ***Subscriber's information or Registration information*** refers to any information contained in the form of computer data or any other form that is held by a service provider or internet intermediary, relating to subscribers or registrants of its services other than traffic or content data and by which any of the following can be established:

(1) The type of communication service used, the technical provisions taken thereto and the period of service;
(2) The identity, postal or geographic address, telephone or other access numbers, assigned network address, billing and payment information of the subscriber or registrant that is available on the basis of the service agreement, arrangement, or registration; and
(3) Any other available information on the basis of the service agreement, arrangement, or registration that may help identify the subscriber or registrant, including the site of the installation of communication equipment.

(ll) ***Supplementary learning and youth activity center*** refers to any public or private establishment, facility, organization, or program that provides instructional, recreational, developmental, or skills-based activities for children or youth outside the formal basic or higher education system.

This includes, but is not limited to, tutorial or review centers, enrichment or learning hubs, sports, arts, or music clinics, computer or language centers, summer camps, after-school programs, community youth centers, libraries with learning programs, and similar venues where minors participate in supervised activities either physically or online.

(mm) ***Technology platforms*** refer to any software application, digital service, or integrated hardware–software system which is designed and made available to users to enable them to create, generate, capture, edit, store, process, transmit, share, publish, distribute, recommend, organize, or otherwise interact with digital content, communications, or data, whether operating online or offline and whether network-connected or stand-alone.

For purposes of this Act, the term includes, among others:

(1) Operating Systems and device environments, and application stores or digital marketplaces through which users obtain or update applications and digital services;

(2) User-facing applications and services that support user-generated content or communications, including social media and content-sharing services, messaging and file-transfer applications, online forums, and games or virtual worlds with user-generated content or communications between users;
(3) Content-generation and editing tools, including image, audio, and video editing software, generative artificial intelligence (AI) models and systems, and other tools capable of producing or manipulating realistic visual, audio, or textual representations of a child; and
(4) Cloud hosting services, content-delivery networks, and software development kits or application programming interfaces (SDKs/APIs) that provide materially similar functionality to the foregoing or embed such functionality into third-party services.

It covers any natural or juridical person that designs, develops, operates, controls, provides, or makes such platform available in or into the Philippines, whether or not it has a physical presence in the country.

(nn) ***Traffic data or non-content data*** refers to any computer data other than the content of the communication, including but not limited to, the origin, destination, route, time, date, size, duration, or type of communication of the underlying service.

(oo) ***Virtual asset*** refers to any type of digital unit that can be digitally traded, or transferred, and can be used for payment or investment purposes. It can be defined as a 'property,' 'proceeds,' 'funds or other assets,' and other 'corresponding value.' It is used as a medium of exchange or a form of digitally stored value created by agreement within the community of virtual asset users.

Virtual assets shall be broadly construed to include digital units of exchange that:

(1) Have a centralized repository or administrator;
(2) Are decentralized and have no centralized repository or administrator; or
(3) May be created or obtained by computing or manufacturing effort.

Virtual assets are not issued nor guaranteed by any jurisdiction and do not have legal tender status.

(pp) ***Virtual asset service provider (VASP)*** refers to any entity that offers services or engages in activities that provide facility for the transfer or exchange of virtual asset, which involve the conduct of one or more of the following activities:

(1) Exchange between virtual assets and fiat currencies;
(2) Exchange between one, or more forms of virtual assets;
(3) Transfer of VAs; and
(4) Safekeeping and/or administration of virtual assets or instruments enabling control over VAs.

(qq) ***Web hosting provider*** refers to a person that provides infrastructure for hosting, supplies web server space and internet connectivity that enables a user to post, upload, download and share user-generated content, or a content provider who supplies content to the Internet. It shall also refer to a person that provides specialized hosting services such as streaming services or application hosting, domain name registration services, or services that enable users to create and manage their websites.

CHAPTER II
PROHIBITED ACTS AND CRIMINAL LIABILITIES

SEC. 4. *Unlawful or Prohibited Acts.* – Regardless of the consent of the child, it shall be unlawful for any person to commit the following acts through online or offline means or a combination of both:

(a) To solicit, hire, employ, use, persuade, induce, extort, engage, maintain, or coerce a child to perform or participate in any manner in the creation, production, or performance of any form of CSAEM;

(b) To produce, direct, manufacture, facilitate, or create any form of CSAEM, or participate in the production, direction, manufacture, facilitation or creation of the same;

(c) To offer, sell, distribute, advertise, promote, export, or import, by any means, any form of CSAEM including sharing on other means of online or offline communication;

(d) To knowingly publish, transmit, share, display or broadcast, by any means, any form of CSAEM;

(e) To permit, allow, tolerate, or otherwise enable a child, including a child under one's care, custody, control, supervision, or influence, to engage in, participate in, or assist in the creation, production, transmission, dissemination, performance, or streaming of any form of CSAEM;

(f) To direct, hire, employ, or provide any consideration to, monetary or otherwise, any person to stream or livestream acts of child sexual abuse or exploitation;

(g) To stream or livestream acts of, or any form of, child sexual abuse or exploitation;

(h) To recruit, transport, transfer, harbor, provide, or receive a child for the purpose of involving or using the child, directly or indirectly, in any capacity, in the creation, production, performance, facilitation, transmission, dissemination, or livestreaming of any form of CSAEM;

(i) To introduce, arrange, or otherwise facilitate, whether through online or offline means or a combination of both, the communication, meeting, or contact of a child with a foreign national or any person for the purpose of subjecting the child to sexual abuse or sexual exploitation, or of involving the child in the creation, production, performance, transmission, dissemination, or livestreaming of any form of CSAEM;

(j) For film distributors, theaters, exhibitors, and internet intermediaries, by themselves or in cooperation with others, to distribute, exhibit, display, transmit, disseminate, host, make available, or otherwise facilitate access to any form of CSAEM, where such act is done knowingly, with willful blindness, or by gross negligence.

For purposes of this paragraph, "willful blindness" refers to the conscious and deliberate avoidance of knowledge of facts or circumstances, despite awareness of a high probability of their existence, in order to deny knowledge or avoid liability under this Act; while "gross negligence" refers to a serious failure to exercise even slight care despite facts or circumstances that would place a reasonably prudent person or entity on notice that CSAEM is being distributed, exhibited, displayed, transmitted, disseminated, hosted, made available, or otherwise facilitated through its services, facilities, or infrastructure.

(k) To offer, advertise, or make available any child for prostitution to another person by, through, or with the use of ICT.

For purposes of this paragraph, the offense is likewise committed where the person represented, advertised, or made available as a child is in fact an adult or where no actual child exists, provided that the offender represents, presents, or otherwise holds out such person or purported person as a child, as defined in this Act, for purposes of prostitution.

(l) To procure, solicit, or pay for the sexual services of a child who is offered, advertised, or made available for prostitution by, through, or with the use of ICT, whether or not the act of sexual exploitation is consummated.

For purposes of this paragraph, the offense is committed regardless of the consent or apparent consent of the child or of any intermediary, and whether monetary or non-monetary consideration, favor, or benefit is given, promised, or received in exchange for the sexual act or the opportunity to commit such act.

The offense under this paragraph is likewise committed where the person offered, advertised, or made available as a child is in fact a law enforcement officer, or another adult posing or represented as a child, or where no actual child exists.

(m) To solicit any person, including a law enforcement officer posing as a child or as a parent or guardian of a child, to create, produce, manufacture, transmit, distribute, publish, broadcast, sell, stream, livestream CSAEM or to commit OSAEC.

The offense under this paragraph shall be consummated by the act of solicitation or attempted solicitation, whether made in person or through any means of ICT, and whether or not the underlying CSAEM or OSAEC offense is in fact carried out or completed;

(n) To commit sexual extortion of a child as defined in Section 3 of this Act;

(o) To knowingly benefit from, financial or otherwise, the commission of any of the offenses of this Act;

(p) For any owner, lessor, operator, manager, or person who has control over any place, building, structure, vehicle, or other venue, to knowingly, including through willful blindness, or by gross negligence, allow, permit, or make available such venue for the commission of any of the prohibited acts under this section, such as, but not limited to, dens, private rooms, cubicles, cinemas, houses, private homes, or other establishments.

For purposes of this paragraph, "willful blindness" refers to the conscious and deliberate avoidance of knowledge of facts or circumstances that would place a reasonably prudent person on notice of a high probability that prohibited acts under this Act are being committed, facilitated, or are likely to be committed in such place, building, structure, vehicle, or other venue, in order to deny knowledge or avoid liability. "Gross negligence" refers to a serious failure to exercise even slight care where, under the facts and

circumstances, a reasonably prudent person would have reason to suspect that prohibited acts under this Act are being committed, facilitated, or are likely to be committed therein, and such person fails to take reasonable measures to verify, prevent, stop, or report such use;

(q) To engage in the luring or grooming of a child as defined in Section 3 of this Act;

(r) To engage in the sexualization of a child as defined in Section 3 of this Act;

(s) To engage in pandering as defined under this Act;

(t) To subscribe to, join, donate to, or support an internet site, platform, service, channel, group, account, or individual for the purpose of obtaining access to, enabling, or funding OSAEC or livestreaming of child sexual abuse and exploitation, or to any site, platform, service, channel, group or individual that the person knows, or should have reasonably known, is primarily dedicated to hosting, offering, marketing, or facilitating OSAEC or CSAEM;

(u) To design, develop, configure, or knowingly distribute any technology platform, AI model, software application, or digital service that is specifically configured, fine-tuned, or optimized for the primary purpose of generating, facilitating, or disseminating CSAEM or CSAEM deepfakes, whether or not any CSAEM has been produced using such platform at the time of the offense: *Provided,* That this prohibition shall not apply to the development or deployment of tools, classifiers, or systems specifically designed and used in good faith for the detection, identification, or suppression of CSAEM;

(v) To advertise, publish, print, broadcast or distribute, or cause the advertisement, publication, printing, broadcasting or distribution by any means of any brochure, flyer, or any material that promotes OSAEC and child sexual abuse or exploitation materials;

(w) To possess any form of CSAEM: *Provided,* That possession of three (3) or more CSAEMs is *prima facie* evidence of the intent to sell, distribute, publish or broadcast;

(x) To willfully access any form of CSAEM;

(y) To conspire to commit any of the prohibited acts stated in this section;

(z) To dissuade a victim, a witness, or the parent, guardian, or a person having control over the victim or witness to report or initiate a complaint for any violations of this Act; and

(aa) For any government official or employee, whether elective or appointive, to facilitate, arrange, initiate, or participate in any meeting, mediation, negotiation, or similar intervention between the child victim or the child's family and the alleged offender or any person acting on behalf of the offender for the purpose of settling, compromising, or otherwise discouraging, preventing, delaying, or causing the non-filing, non-referral to competent authorities, withdrawal, or non-pursuit of a complaint or criminal action for any violation under this Act.

Provided, That the investigation or prosecution of offenses under this Act shall be without prejudice to appropriate investigation and prosecution mechanisms under Republic Act No. 9208, otherwise known as the "Anti-Trafficking in Persons Act of 2003," as amended, and other related laws;

Provided, further, That nothing in this section shall be construed to penalize acts lawfully undertaken pursuant to a court order, lawful and authorized law enforcement operation or investigations, investigations by other agencies authorized to assist law enforcement, legislative hearings, or other authority expressly granted by law.

SEC. 5. *Accomplice Liability.* – Any person who, not being a principal under this Act, knowingly and with intent to facilitate the commission of an offense under this Act, cooperates in its execution by previous or simultaneous acts shall be liable as an accomplice.

Such acts may include, as the case may be, knowingly providing or facilitating access to accounts, devices, platforms, services, payment channels, communication channels, venues, logistical support, technical assistance, moderation, screening, customer support, scheduling, matching, or other means that materially assist the commission, livestreaming, production, distribution, advertising, promotion, sale, purchase, procurement, or sexual exploitation of a child under this Act.

SEC. 6. *Accessory Liability.* – Any person who, with knowledge of the commission of an offense under this Act and without having participated therein as a principal or accomplice, takes part after its commission by any of the following acts shall be liable as an accessory:

(1) Profiting from, assisting the offender to profit from, or knowingly facilitating the retention, transfer, concealment, or enjoyment of the proceeds, instrumentalities, or benefits of the offense;

(2) Concealing, destroying, altering, wiping, transferring, encrypting, or otherwise making unavailable devices, data, records, logs, accounts, storage media, payment records, or other effects or instrumentalities of

the offense in order to prevent its discovery, investigation, or prosecution; or

(3) Harboring, concealing, or assisting in the escape of the principal offender, in the cases allowed under applicable law, without prejudice to a separate criminal prosecution for Obstruction of Justice under P.D. No. 1829.

In the absence of any specific provision to the contrary, the relevant provisions of the Revised Penal Code on accomplices and accessories shall apply suppletorily to offenses punishable under this Act, insofar as they are consistent with the nature, purpose, and provisions of this Act.

SEC. 7. *Syndicated and Large-Scale Violations of this Act.* – Any violation of this Act shall be deemed to have been committed by a syndicate if carried out by a group of three (3) or more persons conspiring or confederating with one another. If the crime was committed against three (3) or more persons, it shall be considered as large-scale violation of this Act.

SEC. 8. *Criminal Sanctions.* – The following penalties shall be imposed on the following offenses:

(a) Any person who violates Section 4, paragraphs (a), (b), (c), (d), (e), (f), (g), (h), (i), (j), (k), and (n) of this Act shall suffer the penalty of life imprisonment and a fine of not less than Two million pesos (P2,000,000.00);

(b) Any person who violates Section 4, paragraphs (o) and (p) of this Act shall suffer the penalty of *reclusión temporal* in its maximum period to *reclusión perpetua* and a fine of not less than One million pesos (P1,000,000.00) but not more than Two million pesos (P2,000,000.00);

(c) Any person who violates Section 4, paragraphs (l) and (m) of this Act shall suffer the penalty of *reclusión temporal* and a fine of not less than Five hundred thousand pesos (P500,000.00) but not more than Two million pesos (P2,000,000.00): *Provided,* That if the sexual act does not occur, the penalty shall be *prisión mayor* and a fine of not less than Two hundred thousand pesos (P200,000.00) but not more than One million pesos (P1,000,000.00);

(d) Any person who violates Section 4, paragraphs (q), (r), and (s) of this Act shall suffer the penalty of *reclusión temporal* in its maximum period and a fine of not less than Eight hundred thousand pesos (P800,000.00) but not more than One million pesos (P1,000,000.00);

(e) Any person who violates Section 4, paragraph (t) of this Act shall suffer the penalty of *reclusión temporal* in its medium period and a fine of not less than Five hundred thousand pesos (P500,000.00) but not more than Eight hundred thousand pesos (P800,000.00);

(f) Any person who violates Section 4, paragraph (u) of this Act shall suffer the penalty of life imprisonment and a fine of not less than Two million pesos (P2,000,000.00) but not more than Ten million pesos (P10,000,000.00);

In addition, the court shall order the forfeiture in favor of the government of any hardware, servers, domains, subdomains, hosting accounts, repositories, model weights, training or fine-tuning datasets, storage media, devices, wallets, digital accounts, payment accounts, proceeds, and other instrumentalities or effects of the offense, without prejudice to the rights of innocent third persons in good faith;

The court may also order the permanent disqualification of the offender from owning, operating, managing, developing, administering, or directly participating in any technology platform, digital service, or online business of a similar nature, where warranted by the gravity of the offense;

(g) Any person who violates Section 4, paragraph (v) of this Act shall suffer the penalty of *reclusión temporal* in its minimum period and a fine of not less than Three hundred thousand pesos (P300,000.00) but not more than Five hundred thousand pesos (P500,000.00);

(h) Any person who violates Section 4, paragraph (w) of this Act shall suffer the penalty of *reclusión temporal* and a fine of not less than Three hundred thousand pesos (P300,000.00) but not more than Five hundred thousand pesos (P500,000.00);

(i) Any person who violates Section 4, paragraph (x) of this Act shall suffer the penalty of *prisión mayor* in its maximum period and a fine of not less than Two hundred thousand pesos (P200,000.00) but not more than Three hundred thousand pesos (P300,000.00);

(j) Any person who violates Section 4, paragraph (y) of this Act shall suffer the penalty of *prisión mayor* in its medium period and a fine of not less than One hundred thousand pesos (P100,000.00) but not more than Two hundred thousand pesos (P200,000.00);

(k) Any person who violates Section 4, paragraph (z) of this Act shall suffer the penalty of *prisión correccional* in its maximum period and *prisión mayor* in its medium period;

(l) Any government official or employee who violates paragraph (aa) of Section 4 of this Act shall suffer the penalty of *prisión correccional* in its maximum period to *prisión mayor* in its minimum period and a fine of not less than Five hundred thousand pesos (P500,000.00) but not more than One million pesos (P1,000,000.00);

In addition, the offender shall suffer the penalty of temporary absolute disqualification from public office and forfeiture of retirement benefits, without prejudice to administrative liability under existing civil service laws, rules, and regulations;

(m) Any person who violates the confidentiality of information imposed on Sections 27, 28, 29, and 30 of this Act shall suffer the penalty of *prisión correccional* in its medium to *prisión mayor* in its minimum and a fine of not less than Five hundred thousand pesos (P500,000.00) but not more than One million pesos (P1,000,000.00). If the offender is a public official or employee, they shall, in addition to the penalties prescribed herein, suffer the penalty of perpetual or temporary disqualification from public office, as the case may be;

(n) Any person covered by the Philippine Child Sex Offenders Registry who fails or refuses to register or update their registration or comply with any of the obligations required under this Act and its implementing rules shall suffer the penalty of *prisión correccional* in its medium to *prisión mayor* in its minimum and a fine of at least One hundred thousand pesos (P100,000.00) but not more than Three hundred thousand pesos (P300,000.00);

(o) Any person who violated the confidentiality provision in Section 24 of this Act shall suffer the penalty of *prisión correccional* in its medium to *prisión correccional* in its maximum;

(p) Any person found guilty of violating Sections 27, 28, 29, and 30 of this Act shall suffer the penalty of *prisión mayor* in its medium period and a fine of not less than Two million pesos (P2,000,000.00) but not more than Five million pesos (P5,000,000.00) for the first offense. In case of subsequent offense, the penalty shall be a fine of not less than Five million pesos (P5,000,000.00) but not more than Ten million pesos (P10,000,000.00) and revocation of its license or franchise to operate and the immediate closure of the establishment, when applicable;

Where the offender is a juridical person, the penalty prescribed for the violation shall be imposed upon the owner, partner, member of the board of directors, trustee, manager, compliance officer, or other responsible officer who:

(1) Directly participated in, authorized, ordered, or knowingly facilitated the commission of the violation;

(2) Had actual knowledge of the violation and, despite having the authority, duty, or ability to prevent, stop, report, or remedy it, knowingly permitted, tolerated, concealed, or failed to act upon it;

(3) Deliberately avoided knowledge of facts that would have made the violation apparent, despite clear warning signs, internal reports, official notices, compliance findings, or other circumstances requiring action; or

(4) Through gross negligence, failed to exercise reasonable supervision, diligence, or control to prevent, stop, report, or remedy the violation;

(q) Unless otherwise stated in this Act, any government official or employee or agent who abuses the authority provided for under Sections 27, 28, 29, and 30 of this Act shall be penalized with imprisonment of *prisión mayor* in its maximum period and perpetual disqualification to hold public office, the right to vote and participate in any public election, and a fine of not less than Five hundred thousand pesos (P500,000.00) but not more than One million pesos (P1,000,000.00). All the benefits due from service in the government of such public officer or employee shall also be forfeited;

(r) If any of the offenses under this Act was committed in large-scale or by a syndicate as defined in Section 7 of this Act, the penalty to be imposed shall be one (1) degree higher;

(s) When the offender is a parent, guardian, or person exercising parental authority or substitute parental authority over the child victim, and is convicted of any offense under this Act involving the exploitation, prostitution, trafficking, production, creation, facilitation, or livestreaming of child sexual abuse or exploitation materials or any other form of child sexual abuse or exploitation, the court shall, in addition to the penalties provided herein, order the permanent deprivation or, where appropriate, suspension of parental authority over the child;

The court shall determine the appropriate measure taking into account the best interests of the child, without prejudice to the application of relevant provisions of the Family Code, Republic Act No. 7610 otherwise known as the "Special Protection of Children Against Abuse, Exploitation and Discrimination Act," and other child protection laws;

The appropriate social welfare agency shall ensure the immediate provision of protective custody, rehabilitation, and alternative care arrangements for the child, consistent with existing laws and regulations;

(t) Unless otherwise provided in this Act, the penalty for an accomplice under this Act shall be one (1) degree lower than the penalty prescribed for the principal offense in the stage in which it was committed, whether consummated, frustrated, or attempted;

(u) Unless otherwise provided in this Act, the penalty for an accessory under this Act shall be two (2) degrees lower than the penalty prescribed for the principal offense in the stage in which it was committed, whether consummated, frustrated, or attempted;

(v) Unless otherwise provided in this Act, the penalty next lower in degree than that prescribed by law for the consummated felony shall be imposed upon the principal in a frustrated felony;

(w) Unless otherwise provided in this Act, a penalty lower in degree by two (2) degrees than that prescribed by law for the consummated felony shall be imposed upon the principal in an attempt to commit the felony;

(x) Solely for purposes of graduating penalties under this Act, where the principal penalty prescribed is life imprisonment, the corresponding penalty in the graduated scale shall be determined by treating life imprisonment as equivalent to *reclusión perpetua*; and

(y) In addition to the above penalties, the following offenders shall be ineligible for parole:

(1) An offender who is a recidivist;
(2) An offender who is a step-parent or collateral relative within the third (3^{rd}) degree of consanguinity or affinity having control or moral ascendancy over the child;
(3) Any offender whose victim died or suffered permanent mental, psychological or physical disability; and
(4) An offender who is a public officer or employee.

SEC. 9. *Confiscation and Forfeiture of the Proceeds, Tools and Instruments Used in Child Sexual Abuse or Exploitation.* – In addition to the penalty imposed for violations of this Act, the court shall order the confiscation and forfeiture in favor of the government of all the proceeds, tools and instruments used in the commission of the crime, unless these are properties of a third person not liable for the unlawful act: *Provided,* That all awards for damages shall be taken from the personal and separate properties of the offender: *Provided, however,* That if such properties are insufficient, the deficiency shall be taken from the confiscated and forfeited proceeds, tools and instruments.

All proceeds derived from the sale of properties used for the commission of any form of child sexual abuse or exploitation shall be exclusively used for the purpose of child-rearing programs under the special account of the Department of Social Welfare and Development (DSWD).

When the proceeds, tools and instruments used in the commission of the offense have been destroyed, diminished in value or otherwise rendered worthless by any act or omission, directly or indirectly, of the offender, or it has been concealed, removed, converted or transferred to prevent the same from being found or to avoid forfeiture or confiscation, the offender shall be ordered to pay the amount equal to the value of the proceeds, tools and instruments used in the commission of the offense.

SEC. 10. ***Alien Offenders.*** – If the offender is a foreigner, the offender shall be criminally prosecuted immediately. Thereafter, the offender shall be deported after serving sentence and will be permanently barred from re-entering the Philippines.

SEC. 11. ***Effect of Consent of the Victim.*** – The consent of the victim is not material or relevant and shall not be available as a defense in the prosecution of the unlawful acts prohibited under this Act.

No parent, guardian, or person exercising parental authority or acting in loco parentis shall have the legal capacity to consent to, authorize, acquiesce in, or facilitate any act constituting OSAEC or CSAEM on behalf of a minor. Any purported consent, authorization, or acquiescence to such act by any such person shall be void ab initio and shall not constitute a defense in any civil, criminal, or administrative proceeding under this Act.

SEC. 12. ***Good-Faith Reporting and Safe Harbor Exceptions.*** –

(a) **Good-Faith Reporting.** – Any person who, in good faith, reports suspected OSAEC, CSAEM, or related technology-facilitated child sexual abuse or exploitation to competent authorities, authorized reporting channels, hotlines, clearinghouses, covered entities, or other mechanisms recognized under this Act shall not be held civilly, criminally, or administratively liable by reason only of such report.

(b) **Strictly Necessary and Authorized Handling.** – The strictly necessary access to, possession of, review, analysis, classification, hashing, redaction, forensic preservation, secure storage, secure internal transmission, or turnover of CSAEM shall not give rise to civil, criminal, or administrative liability under this Act or other applicable laws, but only when undertaken:

(1) To comply with duties expressly required under this Act or the implementing rules and regulations;

(2) To report or turn over CSAEM to competent authorities or authorized reporting systems;

(3) For the investigation, prosecution, adjudication, or other lawful administration of criminal justice, by or under the direct authority of competent authorities;

(4) For the preparation of a journalistic, documentary, or public-affairs report on a matter of legitimate public concern, but only with respect to text-based, chat-based, or other purely written CSAEM, and only through the review of victim-provided written materials, message records, chat transcripts, lawfully issued court records, official statements, or lawfully redacted derivatives thereof, strictly to the extent necessary for such purpose: *Provided,* That this paragraph shall not authorize access to, possession of, copying of, storage of, transmission of, or republication of any image-based or video-based CSAEM, nor the unnecessary retention, reproduction, or dissemination of written CSAEM beyond what is strictly necessary for immediate reporting, verification, or turnover to competent authorities; or

(5) For duly approved policy, scholarly, or academic research under a specific project approved by a duly constituted and recognized ethics review board, and subject to such further written authority as may be required under this Act or the implementing rules and regulations: *Provided,* That this paragraph shall not authorize independent access to, possession of, copying of, retention of, or use of image-based or video-based CSAEM except upon express legal authority, court order, or written authority from the competent government authority, and only to the minimum extent strictly necessary for the approved purpose.

For purposes of paragraph (b), the exemption shall extend only to the acts expressly enumerated herein and shall not include publication, republication, re-uploading, personal retention beyond what is strictly necessary, sharing outside the authorized chain, or any act not indispensable to a purpose expressly stated in this section.

This exemption shall apply only where the act is strictly necessary and lawful, the handling is limited to the minimum extent reasonably required, appropriate safeguards on minimization, restricted access, secure handling, logging, non-republication, and prompt turnover or deletion are observed, and the act is not for sexual gratification, commercial exploitation, promotion,

dissemination, publicity, entertainment, content creation, or any unauthorized purpose.

A claim of journalistic, documentary, public-affairs, scholarly, academic, research, or content-creation purpose shall not, by itself, be sufficient to qualify for the exemption under this section.

(c) **Good-Faith Child Protection Interventions.** – Any law enforcement officer, social welfare officer, health personnel, or authorized representative of a government agency or accredited non-government organization who, in good faith and in the performance of official duties or authorized functions under this Act, conducts or participates in rescue operations, protective custody, case management, referral, or other lawful interventions for the protection of a child shall be free from administrative, civil, or criminal liability arising therefrom.

Such immunity shall not apply in cases of bad faith, gross negligence, or willful violation of the rights of the child or other persons under existing laws.

(d) **Strictly Necessary Handling of Materials for Safety Systems Addressing CSAEM and OSAEC-Related Activities.** – Access to, possession of, or other strictly necessary handling of materials by covered entities and competent authorities shall not give rise to civil, criminal, or administrative liability under this Act or other applicable laws, solely to the extent necessary to develop, train, test, validate, or operate a dedicated safety system or process used exclusively for the identification, detection, prevention, disruption, hashing, classification, filtering, blocking, removal, reporting, or suppression of CSAEM or OSAEC-related activities, including grooming, luring, enticement, recruitment, solicitation, or other conduct of a similar nature reasonably indicative of imminent or ongoing OSAEC, whether such systems are automated, machine-assisted, or human-assisted, and subject to reasonable safeguards on necessity, minimization, purpose limitation, secure handling, restricted access, logging, and audit trails, as may be further provided in the implementing rules and regulations: *Provided,* That this paragraph shall apply only to materials that do not depict, identify, originate from, remain traceable to, or permit the reconstruction or re-identification of an actual child, including hashes, metadata, classifications, synthetic or simulated data, and redacted, transformed, or other non-reconstructible image-, video-, audio-, or text-based materials; *Provided, further,* That in no case shall any actual CSAEM, or any material that depicts, identifies, is derived from, is traceable to, or is reasonably capable of reconstructing or re-identifying an actual child, be used, retained, copied, fed into, or otherwise employed under this paragraph; *Provided, finally,* That nothing in this

paragraph shall be construed to authorize public dissemination, republication, commercial exploitation, unrelated model development, or any use beyond what is strictly necessary for the purposes expressly stated herein.

(e) **Rulemaking; Safeguards.** – The implementing rules and regulations shall prescribe the criteria, limitations, and safeguards for the application of this section, including standards on lawful authority, good faith, necessity, minimization, confidentiality, secure handling and storage, redaction, de-identification, access controls, logging, audit trails, retention, turnover, deletion, disposal, and prohibitions against unauthorized republication, dissemination, promotion, or commercial exploitation of CSAEM, recorded forensic interviews, or other protected materials covered by this section.

(f) **Non-Exclusivity.** – The safe harbor exceptions under this section are in addition to, and not in substitution for, any exemption, immunity, or defense otherwise recognized under this Act or other applicable laws.

SEC. 13. ***Prescription of Criminal Actions.*** –

(a) Criminal actions for offenses under this Act punishable by life imprisonment shall be imprescriptible.

(b) All other criminal actions shall prescribe within twelve (12) years, counted from the date of discovery of the offense or from the date the child reaches the age of majority, whichever occurs later.

(c) The filing of a complaint before the prosecutor, law enforcement authorities, or any other competent authority shall interrupt the prescriptive period.

(d) For continuing offenses, including but not limited to grooming, possession, distribution, transmission, or making available of child sexual abuse or exploitation material (CSAEM), the prescriptive period shall run only from the date the unlawful conduct ceases.

(e) Prescription shall not run when the person or any responsible entity has fraudulently concealed the violation or prevented its discovery through deceptive, anonymizing, or obstructive means.

CHAPTER III
INVESTIGATION, PROSECUTION AND CASE HANDLING

SEC. 14. ***Initiation of Investigation.*** – Law enforcement agencies are mandated to immediately initiate investigation and counter-OSAEC and -CSAEM-

intelligence gathering upon receipt of statements or affidavits from victims of OSAEC and CSAEM, or their families, and other persons who have knowledge or information about violations of this Act, including the private sector, as well as referrals from foreign law enforcement.

Agencies that receive complaints of violations of this Act shall develop both online and in person reporting mechanisms that are gender-sensitive, age-appropriate and culturally sensitive to children, especially girls.

SEC. 15. *Authority to Intercept and Record.* – In investigating violations of this Act, a law enforcement officer may, upon a written order from the regional trial court, track, intercept, view, monitor, surveil, listen to, and record, by technical or electronic means, any communications, information or messages, including the procurement of content data, transmitted by means of a computer system involving at least one (1) person reasonably believed to have committed violations under this Act: *Provided,* That when the offense involves the use of computer systems and digital platforms, a court order shall not be required in order for a law enforcement officer acting in an undercover capacity to intercept a communication with a person reasonably believed to have committed, is committing, or is about to commit any of the violations of this Act.

Where an order is required, the order shall only be issued or granted upon written application of a law enforcement officer, who shall be examined under oath or affirmation, and the witnesses the officer may produce and the showing that:

(a) There are reasonable grounds to believe that any of the crimes enumerated hereinabove has been committed, or is being committed, or is about to be committed;

(b) There are reasonable grounds to believe that evidence that will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of, any such crimes; and

(c) There are no other means readily available for obtaining such evidence.

The order shall only be effective for the length of time determined by the court, which shall not exceed a period of ten (10) days from its issuance. The court issuing the order may, upon motion, extend its effectivity based only on justifiable reasons for a period not exceeding ten (10) days from the expiration of the original period.

In investigating violations of this Act involving the use of the Internet and other digital platforms, law enforcement officers acting in an undercover capacity who record their communications with a person or persons reasonably believed to have

committed, is committing, or is about to commit any of the violations under this Act shall not be considered as wiretapping or illegal interception, shall not be liable under the provisions of Republic Act No. 4200, otherwise known as "The Anti-Wiretapping Law": *Provided,* That victims of violations of this Act shall not be liable under the provisions of the Anti-Wiretapping Law and Republic Act No. 10175 otherwise known as the "Cybercrime Prevention Act of 2012" if they record, transmit, or perform any other acts directly or indirectly related to the reporting of any violation of this Act committed against them.

SEC. 16. *Power to Administer Oath and Subpoena.* – The Chief of the Women and Children Protection Center of the Philippine National Police (PNP-WCPC) and the Director of the PNP Anti-Cybercrime Group (PNP-ACG) shall have the power to administer oath, and issue subpoena and subpoena *duces tecum* strictly in relation to its investigation in OSAEC and CSAEM cases: *Provided,* That such power shall be exercised solely by the aforementioned officials and may not be further delegated to any other person or office.

The subpoena shall state the nature and purpose of the investigation and shall be directed to the person whose attendance is required, and in the case of a subpoena *duces tecum*, it shall also contain a reasonable description of the books, documents, digital data, or things demanded which must be relevant to the investigation.

Failure to comply with a lawfully issued subpoena or subpoena *duces tecum* shall authorize the filing of a petition for indirect contempt under the Rules of Court with the appropriate regional trial court.

SEC. 17. *Authority to Conduct Digital Forensic Examination.* – Notwithstanding the provisions of the Cybercrime Prevention Act of 2012 and its implementing rules and regulations, the PNP-WCPC, the National Bureau of Investigation (NBI), and other agencies authorized by this Act or other laws are hereby authorized to conduct computer data recovery and forensic examination, extraction, and analysis of computer systems and other electronic evidence lawfully seized in OSAEC/CSAEM cases.

For this purpose, the PNP-WCPC, NBI and other agencies authorized by this Act or other laws to conduct digital forensic examination shall be capacitated and shall maintain a pool of qualified digital forensic examiners to conduct forensic examination of seized digital devices, in accordance with existing laws, rules, and internationally accepted forensic standards.

SEC. 18. *Who May File a Complaint.* – Complaints on cases of any form of child sexual abuse or exploitation punishable under this Act may be filed by the following:

(a) Offended party, including children whose face and likeness is depicted in the form of synthetic media that is subject of the synthetic complaint;
(b) Parents or guardians of offended party;
(c) Ascendant or collateral relative within the third (3rd) degree of consanguinity;
(d) Officer, social worker or representative of a licensed child-caring institution;
(e) Officer or social worker of the DSWD;
(f) Local social welfare development officer;
(g) Any barangay official;
(h) Any law enforcement officer;
(i) Any authorized officer of a competent authority;
(j) At least three (3) concerned responsible citizens residing in the place where the violation occurred; or
(k) Any person who has personal knowledge of the circumstances of the commission of any offense under this Act.

SEC. 19. *Affidavit of Desistance.* – Cases involving OSAEC and CSAEM shall not be dismissed based on the affidavit of desistance executed by the victims or their parents or legal guardians. Public and private prosecutors are directed to vigorously oppose and manifest objections to motions for dismissal. Any act that unduly pressures the complainant to execute an affidavit of desistance shall be punishable under this Act.

SEC. 20. *Special Procedural Rules for Technology-Facilitated OSAEC and CSAEM Cases.* – Considering the cybercrime and technology-facilitated nature of OSAEC and CSAEM cases, the verified review, examination and analysis by a competent Philippine law enforcement authority of the information lawfully obtained through digital systems, recognized child-protection reporting mechanisms, financial intelligence channels, or official foreign law enforcement agencies, shall constitute personal knowledge for purposes of applying for search warrants, cyber warrants, or other judicial authorizations.

Personal knowledge shall be deemed to include such independently verified information shall not be considered hearsay for purposes of determining probable cause, subject to judicial evaluation and constitutional safeguards.

Where the reviewed and analyzed information transmitted by foreign law enforcement agencies or National Center for Missing and Exploited Children (NCMEC) establishes: (1) the identity of the offender, (2) that the offense is continuing in nature, and (3) delay would endanger a child, the Philippine law enforcement officer may lawfully effect a warrantless arrest on the ground that an offense is being committed, or has just been committed, or is about to be committed, and the officer has personal knowledge of facts indicating that the person to be arrested committed it.

Considering the need for immediate victim identification and safeguarding, digital evidence preservation, forensic examination or analysis, coordination with financial intermediaries, deconfliction of foreign referrals, and coordination with prosecutors and competent authorities, the period for delivery of a person lawfully arrested without warrant for violations of this Act to the proper judicial authorities shall be seventy-two (72) hours, as an exception to Article 125 of the Revised Penal Code. The arrested person shall, at all times, be informed of the cause of arrest and afforded all rights guaranteed under the Constitution, the Rules of Court, custodial investigation laws, and other applicable laws.

SEC. 21. ***Jurisdiction.*** – Jurisdiction over criminal cases for the violation of this Act shall be vested in the Family Court which has territorial jurisdiction over the place where the offense or any of its essential elements was committed, pursuant to Republic Act No. 8369, otherwise known as the "Family Courts Act of 1997": *Provided,* That the court shall not require the presence of a child victim during the trial and that the child shall testify in accordance with the "Rules on Examination of a Child Witness", as may be provided by the Supreme Court and the Rules of Court.

SEC. 22. ***Extraterritorial Jurisdiction.*** – The State shall exercise jurisdiction over any act defined and penalized under this Act, even if all elements of the offense were committed outside the Philippines and whether or not such act constitutes an offense at the place of commission, when:

(a) The offender, suspect, respondent, or accused is a Filipino citizen;
(b) The offender, suspect, respondent, or accused is a permanent resident of the Philippines; or
(c) The victim is a Filipino citizen.

Service of Subpoena and Other Processes – In cases involving foreign, non-resident, or unlocatable respondents, or respondents whose personal service cannot be effected despite reasonable efforts, any subpoena, notice, order, resolution, or other process issued by the prosecutor during inquest, preliminary investigation, reinvestigation, or case build-up proceedings under this Act may be served through the respondent's last known physical address, electronic mail address, mobile number, online account, social media account, messaging application, registered account information, published contact details, known counsel, agent, representative, employer, service provider, or through any verified contact detail or electronic notification channel associated with the respondent's platform, payment wallet, or other registered account, or by any other electronic, substituted, or alternative means reasonably calculated to give notice.

Proof of transmission, delivery, publication, attempted transmission, attempted delivery, or other documented effort to serve the subpoena, notice, order, resolution, or process through such means shall be sufficient for the prosecutor to

proceed with the inquest, preliminary investigation, reinvestigation, or case build-up proceeding and to resolve the complaint based on the evidence on record.

SEC. 23. *Venue.* – A criminal action arising from a violation of this Act shall be filed where the offense was committed, where any of its elements occurred, or where the child is found or actually resides at the time of the commission of the offense: *Provided,* That the court where the criminal action is first filed shall acquire jurisdiction to the exclusion of the other courts.

SEC. 24. *Confidentiality and Protective Measures.* – At every stage of reporting, referral, rescue, protection, investigation, prosecution, trial, service delivery, recovery, reintegration, and aftercare under this Act, the confidentiality, privacy, safety, dignity, and best interests of the child shall be protected.

For this purpose, the following rules shall apply:

(a) The judge, prosecutor, law enforcement officer, social welfare officer, barangay official, teacher, school personnel, health worker, service provider, covered entity, media practitioner, or any other person who receives, handles, refers, investigates, assists, reports on, or acts upon any report, complaint, referral, material, record, or case under this Act shall keep confidential the identity and personal circumstances of the child, the child's family, and any information that may directly or indirectly identify the child;

(b) Information relating to a child, victim-survivor, report, referral, investigation, prosecution, protection intervention, or aftercare service shall be shared only for legitimate child protection, reporting, referral, rescue, investigation, prosecution, case management, service delivery, court-authorized, regulatory, compliance, or other lawful purposes under this Act and other applicable laws;

(c) The name, image, voice, address, school, family circumstances, online identifiers, account information, or any other information tending to establish the identity of the child or the child's immediate family shall not be disclosed to the public, published, broadcast, uploaded, shared online, or otherwise made available through any medium;

(d) The judge, prosecutor, or competent authority may, whenever necessary to ensure a fair and impartial proceeding and after considering the best interests, safety, privacy, and protection of the child, conduct a closed-door investigation, proceeding, or trial, or order the sealing, redaction, anonymization, pseudonymization, or restricted access of records;

(e) Records involving a child shall be confidential and kept under seal. Access may be granted only upon lawful authority, written request, and order of the court, and only to persons whose access is necessary for the administration of justice, child protection, investigation, prosecution, defense of the accused, case management, service delivery, or other lawful purpose, subject to protective conditions imposed by the court;

(f) In no case shall CSAEM be copied, reproduced, furnished, transmitted, downloaded, exported, or provided to the accused, defense counsel, private complainant, media, or any unauthorized person. Where access to CSAEM is necessary to protect the rights of the accused, the court shall allow only controlled access through secure in-camera inspection, supervised viewing, use of certified descriptions, redacted or non-reconstructible derivatives, forensic reports, hashes, summaries, stipulations, or other protective means that preserve the right to a fair trial while preventing republication, redistribution, possession, or further harm to the child;

(g) Any CSAEM, recorded forensic interview, child-victim record, or other protected material forming part of court, prosecutorial, law-enforcement, social welfare, medical, school, referral, or service-provider records shall be subject to a protective order or equivalent confidentiality directive. Such order or directive shall, at a minimum, prohibit copying, reproduction, disclosure, republication, uploading, redistribution, or unauthorized retention; limit access to persons authorized by the court or competent authority; require written acknowledgment of the protective order; and subject any violation to contempt, administrative, civil, criminal, or other liability under applicable laws;

(h) Recorded forensic interviews of children shall not be accessed, viewed, used, reproduced, published, distributed, or retained except for child protection, case management, investigation, prosecution, adjudication, professional supervision, specialized training, or other lawful purposes authorized by the court or competent authority. Any academic, research, training, or instructional use shall require appropriate legal authority, ethics review where applicable, strict necessity, minimization, confidentiality, secure handling, restricted access, de-identification or redaction where practicable, non-republication, and other safeguards prescribed in the implementing rules and regulations;

(i) It shall be unlawful for any editor, publisher, reporter, columnist, announcer, producer, broadcaster, director, social media influencer,

content creator, platform user, or any other person to cause undue publicity, disclosure, commentary, publication, broadcast, upload, sharing, or dissemination that identifies, tends to identify, sexualizes, blames, shames, stigmatizes, or causes further suffering to the child, the child's family, or the victim-survivor; and

(j) Any person or agency involved in the reporting, referral, rescue, protection, investigation, prosecution, trial, service delivery, recovery, reintegration, or aftercare of cases under this Act shall refrain from any act, statement, publication, communication, or disclosure that blames the victim, places responsibility on the victim, trivializes the abuse, or exposes the child to retaliation, stigma, harassment, or further harm.

The confidentiality obligations under this section shall apply without prejudice to the right of the accused to a fair trial, the authority of the court to regulate access to evidence, and the duty of competent authorities to preserve, authenticate, and present evidence in accordance with law.

SEC. 25. ***Applicability of Juvenile Justice and Welfare Act, as Amended.*** – In cases where the offender is a child, the prosecution of the offense shall be in accordance with Republic Act No. 9344, otherwise known as the "Juvenile Justice and Welfare Act of 2006," as amended, and the child shall be accorded the appropriate treatment and services under the said law: *Provided,* That in cases of First-Person Produced CSAEMs, the child producing the sexualized materials shall be considered as a victim and not as an offender. The child victim shall be accorded the necessary treatment and services under this Act and in existing laws.

SEC. 26. ***Appointment of Special Prosecutors.*** – The Department of Justice (DOJ) shall appoint or designate special prosecutors to prosecute cases for the violation of this Act.

Prosecutorial policies, enforcement guidelines, and operational directives issued pursuant to this Act shall ensure equal prioritization and prosecution of trafficking-related and non-trafficking forms of OSAEC and CSAEM.

Non-commercial exploitation, including but not limited to familial abuse, grooming without financial exchange, image-based sexual abuse, coercion, and technology-facilitated exploitation absent monetary transaction, shall receive equal prosecutorial attention and resource allocation.

The DOJ shall develop mechanisms for disaggregated reporting of OSAEC and CSAEM cases by category to monitor enforcement distribution, identify implementation gaps, and support evidence-based policy refinement.

The IRR shall prescribe monitoring standards consistent with due process and prosecutorial independence.

CHAPTER IV
DUTIES OF COVERED ENTITIES

SEC. 27. ***Duties and Responsibilities of Internet Intermediaries, Technology Platforms, Device Manufacturers, Payment Service Providers, and Virtual Asset Service Providers.*** – The following entities shall have the corresponding duties and responsibilities to prevent, detect, report, and disrupt the commission of OSAEC and CSAEM as defined in this Act, without prejudice to their obligations under existing laws and regulations.

(a) Duties Common to Internet Intermediaries, Technology Platforms, Payment Service Providers, and Virtual Asset Service Providers.

The duties under this subsection shall apply to internet intermediaries, technology platforms, PSPs, and VASPs that provide services, systems, tools, products, or functionalities to the public and either:

(i) Provide infrastructure or services that enable users to access, transmit, route, cache, host, store, share, disseminate, index, search for, or otherwise make available third-party content, products, services, or applications on or through the Internet;
(ii) Enable users to create, generate, capture, edit, transform, manipulate, store, process, transmit, share, publish, distribute, recommend, or otherwise interact with digital content, communications, or data, whether online, offline, or through hybrid functionality; or
(iii) Facilitate, process, route, settle, or otherwise enable digital payments or other financial transactions linked to user activity, content, access, or services.

(1) Prevent, Reduce, Mitigate, and Disrupt OSAEC and CSAEM Risks. – Take reasonable, proportionate, technically feasible, and context-appropriate measures to prevent, reduce, mitigate, and disrupt foreseeable risks that their services, systems, products, features, user-interaction tools, payment channels, or business practices may be used to commit, facilitate, amplify, monetize, conceal, or perpetuate OSAEC, CSAEM, or related technology-facilitated child sexual abuse or exploitation.

In determining compliance with this duty, due regard shall be given to the nature, size, scale, reach, functionality, technical architecture, level of control, user base, transaction volume, risk profile, and role of the covered

entity in the commission, facilitation, detection, prevention, disruption, reporting, or investigation of OSAEC, CSAEM, or related technology-facilitated child sexual abuse or exploitation.

The specific duties under this section and Section 28 are without prejudice to the obligation of covered entities to adopt other reasonable, proportionate, technically feasible, and context-appropriate measures necessary to address foreseeable OSAEC and CSAEM risks.

(2) Terms of Service, User Agreements, and Product-Use Restrictions. – Prohibit, in their terms of service, end-user license agreements, terms of use, developer terms, service agreements, merchant agreements, account terms, wallet terms, or equivalent user, contractual, or product documentation, the use of their platforms, services, systems, tools, or products for OSAEC, CSAEM, or any act prohibited under this Act, including but not limited to the sexualization of children; the creation, generation, manipulation, distribution, or other facilitation of AI-generated or digitally manipulated sexual depictions or representations of children; and other sexual depictions or representations of children, and shall implement and enforce such prohibitions in a consistent, accessible, and auditable manner.

(3) Reporting Channel for OSAEC and CSAEM Concerns and Correction Channel. – Maintain to the extent possible, user-facing, customer-facing, merchant-facing, or other publicly accessible digital interfaces, websites, applications, dashboards, portals, or support channels, establish and maintain an easily accessible reporting channel or link through which users, civil-society organizations, merchants, business users, and competent authorities may notify the covered entity that its platform, service, system, tool, product, or feature is being used for OSAEC or CSAEM. The reporting channel shall be clearly visible, in plain language, and easy to follow and use.

They shall likewise provide an accessible mechanism for requesting review or correction of manifest error in blocking, removal, restriction, suspension, delisting, or other action taken under this Act, consistent with child protection, confidentiality, evidence preservation, and the needs of investigation and prosecution.

(4) Public-Facing Child Safeguarding Information. – Provide product documentation, help files, websites, applications, dashboards, portals, onboarding materials, or other reasonably accessible means, make available clear information on:

(i) The prohibition on using the platform, service, system, tool, or product for CSAEM or the sexualization of children; and

(ii) Any built-in safety features designed to prevent such misuse.

(5) Child Protection and Safeguarding Standards and Policies. – Adopt and integrate child protection standards and policies in their corporate governance practices, safety systems, trust and risk mechanisms, and operational processes, in a manner appropriate to the nature of their services, systems, tools, products, or functionalities.

(6) Age Assurance and Age Verification Protocols. – Implement age assurance or age verification protocols before granting users access to covered age-restricted content, services, accounts, products, or features.

Covered age-restricted content, services, accounts, products, or features shall include those that may expose children to: a) OSAEC, CSAEM, or related technology-facilitated child sexual abuse or exploitation; (b) grooming, sexual solicitation, sexual extortion, livestreamed sexual abuse, or other sexual exploitation risks; (c) adult sexual, pornographic, sexually explicit, or monetized sexual content; (d) interactive or recommender features that may facilitate child sexual abuse or exploitation and (e) payment wallet, virtual asset, merchant, monetization, or other financial services that may facilitate, monetize, conceal, or transmit proceeds of such abuse or exploitation. Mere self-declaration, tick-box confirmation, or entry of date of birth shall not be sufficient unless supported by additional measures appropriate to the nature of the content, service, account, product, or feature.

The NCC, in coordination with the Department of Information and Communications Technology (DICT), National Telecommunications Commission (NTC), National Privacy Commission (NPC), DOJ-Office of Cybercrime (DOJ-OCC), and *Bangko Sentral ng Pilipinas*, and other relevant authorities, shall promulgate the necessary rules, technical standards, and guidelines for the implementation, certification, audit, reporting, interoperability, and enforcement of this section, ensuring that all adopted age assurance and verification are highly effective, proportionate, and compliant with existing data privacy laws, without mandating sensitive personal information and data processing mechanisms.

(7) Notification of OSAEC and CSAEM Activity. – Notify the NC-COpS and provide such information as may be required under this Act and its implementing rules and regulations within forty-eight (48) hours from

receipt of information, acquisition of actual knowledge, or awareness of facts and circumstances reasonably indicating that OSAEC and/or CSAEM is being committed, facilitated, or attempted through, by means of, or using its platform, service, system, facility, or financial channels.

NC-COpS shall refer, transmit, or provide access to such reports to the appropriate law enforcement, prosecutorial, regulatory, child-protection, or international-cooperation authority, as the circumstances may require.

The processing and disclosure of information pursuant to this paragraph shall constitute lawful processing under Republic Act No. 10173, or the "Data Privacy Act of 2012."

(8) Foreign-Law Restricted Disclosure and NCC Routing. – Where a foreign covered entity is, by reason of its domestic law or binding governmental policy, prohibited from directly disclosing certain data, information, or evidence to Philippine authorities, any reporting or notification obligation under this Act shall be deemed complied with respect to such restricted data, information, or evidence if the relevant report or notification is made through the mechanisms recognized under Section 65 of this Act on foreign referrals, cybertipline reports, and international hotlines, or through the corresponding authority, body, cybertipline, hotline, clearinghouse, or analogous entity in its jurisdiction that has existing arrangements, protocols, or recognized channels for transmitting the same, or its substance, to Philippine authorities.

Any data, information, or evidence not prohibited from direct disclosure shall nevertheless be furnished or made available to the NCC in accordance with this Act.

The NC-COpS shall, without undue delay, furnish to, or provide access for, such other competent authorities and agencies as may be deemed appropriate under the circumstances any report, notification, information, or data received under this Act that may require referral, coordination, investigation, preservation, enforcement, or other appropriate action.

Nothing in this paragraph shall impair the functions of the DOJ-OOC, DOJ, law enforcement agencies, or other competent authorities under existing cybercrime, mutual legal assistance, police-to-police, or international cooperation mechanisms.

(9) Requirement for Non-Notification Clause. – Incorporate a strict non-notification policy into terms of service or equivalent documentation of covered entities that maintain account, subscription, licensing, merchant, digital wallet, or comparable contractual relationships. This proviso shall expressly prohibit the entity from directly or indirectly notifying any relevant person—including account holders, subscribers, or merchants—who are implicated, linked, or reasonably suspected in an OSAEC or CSAEM investigation. Specifically, the entity must not disclose the existence, contents, or status of any preservation request, *subpoena*, cybercrime warrant, court order, takedown directive, freeze measure, or other lawful governmental request served under this Act for criminal investigation purposes.

(10) Undercover Investigative Accounts and Cooperative Arrangements. – In accordance with this Act and subject to safeguards prescribed in the implementing rules and regulations, enter into arrangements, protocols, or other lawful cooperative mechanisms with competent authorities for the creation, maintenance, use, preservation, non-disruption, or confidential handling of undercover accounts, profiles, pages, channels, wallets, merchant accounts, payment instruments, or other comparable digital presences or instruments for lawful investigation, intelligence development, surveillance, or case build-up under this Act.

Such arrangements or protocols shall provide for appropriate authorization, designated focal persons, confidentiality, restricted access, documentation, oversight, and procedures for suspension, discontinuance, or closure, and shall ensure that the use of such undercover accounts or instruments is limited to lawful purposes under this Act and other applicable laws.

No covered entity or platform, and no responsible officer, employee, or personnel thereof, shall be held civilly, criminally, or administratively liable solely by reason of good-faith compliance with such arrangement, protocol, or lawful directive under this Act, including the creation, maintenance, continued use, preservation, or non-disruption of undercover accounts, profiles, pages, channels, wallets, merchant accounts, payment instruments, or other comparable digital presences or instruments.

(11) Single Electronic Point of Contact. – Maintain a single electronic point of contact for competent authorities and regulators for notices, reports, preservation requests, subpoenas, warrants, court orders, compliance communications, and other lawful processes under this Act, in the manner prescribed by the implementing rules and regulations.

(12) Execution Records. – Covered entities shall, where applicable, maintain tamper-evident records of notices, reports, requests, or orders received under this Act, including the date and time of receipt, action taken, date and time of execution, preservation measures taken, and grounds for any non-execution or delayed execution, in accordance with the retention periods and safeguards prescribed in the implementing rules and regulations.

(b) Additional Duties of Internet Intermediaries and Technology Platforms.

In addition to those provided in paragraph (a), internet intermediaries and technology platforms shall:

(i) Preservation of Subscriber or Registration Information, Traffic Data, and Content Data. – Preserve subscriber or registration information, traffic data, and content data in a manner that ensures authenticity and integrity, for the following periods:

(1) Subscriber or registration information – within one (1) year from the date of the transaction, extendible for another one (1) year; and

(2) Content Data – within one (1) year upon notice by a law enforcement officer or by a competent authority, extendible for one (1) year.

(ii) Blocking, Removal, Takedown, or Restriction. – Immediately block access to, remove, take down, disable, delist, restrict, or otherwise prevent access to or use of any internet address, URL, website, profile, page, channel, account, or application:

(1) containing any content thereof that constitutes CSAEM or through which any form of OSAEC is being committed, within twenty-four (24) hours from receipt of notice containing sufficient information to identify the content and its source from a competent authority;

(2) containing any content thereof that constitutes CSAEM or through which any form of OSAEC is being committed, within twenty-four (24) hours from actual knowledge of the internet intermediary or technology platform of the existence of any CSAEM content or OSAEC activity being committed in or through its platforms, services, servers, or facilities;

(3) containing any content thereof that constitutes apparent CSAEM, within twenty-four (24) hours from receipt of notice containing sufficient information to identify the content and source thereof from any person or entity; or

(4) containing any content through which any other form of OSAEC not covered in paragraph (iii) is being committed, within forty-eight (48) hours from receipt of notice containing sufficient information to identify the content and source from any person or entity.

Provided, That the obligation to preserve subscriber or registration information, traffic data, and content data under paragraph (1) of this subsection shall continue to apply notwithstanding such blocking, removal, takedown, disablement, delisting, or restriction under this paragraph.

(iii) Reporting of Blocked, Removed, or Restricted Content or Activity. – Within three (3) days from blocking, removal, takedown, or restriction under the immediately preceding paragraph, submit a report to the NC-COpS, identifying the internet addresses, URLs, websites, accounts, applications, content, assets, or services so blocked, removed, taken down, disabled, delisted, restricted, or otherwise acted upon, and stating that the basis for such action is OSAEC and/or CSAEM under this Act.

The report shall also indicate, where applicable, whether the content, account, activity, asset, or service appears to involve imminent harm, ongoing abuse or exploitation, identifiable victims or offenders, immediate preservation needs, financial transactions or monetization, repeat offending, or other circumstances that may warrant urgent investigative, prosecutorial, or international-cooperation action.

Provided, That submission of such report to Philippine-accredited or recognized cybertiplines, hotlines, or clearinghouses that are required to transmit the same, or provide access thereto, to the NC-COpS or Philippine authorities shall be deemed compliance with the foregoing requirement.

(iv) Systems, Designs, Measures, and Procedures. – Develop, implement, maintain, and periodically review technical and organizational systems designed to prevent, detect, report, and respond to OSAEC and CSAEM within their platforms and services, including, where appropriate and proportionate, the use of automated tools. Such systems shall meet the baseline standards

established by the NTC and DICT in coordination with other NCC member agencies. No covered entity may refuse to adopt such systems solely on the ground that violations occur through private or encrypted messaging, where technology is available to do so in a manner consistent with applicable privacy, data protection, and other relevant laws. Nothing in this Act shall be construed to require breaking, weakening, bypassing, or creating backdoors to end-to-end encryption.

Internet intermediaries and technology platforms shall submit to such audit, assessment, reporting, or independent verification requirements as may be prescribed in the implementing rules and regulations.

(v) Safety-by-Design Controls. – Implement effective and proportionate safety-by-design controls, commensurate to the nature of their services and the risks of OSAEC and CSAEM presented thereby, including—where appropriate—default settings protective of minor users, restrictions on profiling of minors for targeted advertising, and safeguards against the generation, transmission, or dissemination of CSAEM. The specific controls shall be prescribed by the NCC, through the joint recommendation of NC-COpS, DICT, and NTC, having regard to internationally recognized age-appropriate design standards.

(vi) Training, Fine-Tuning, Evaluation, and Model Safety Processes. – Internet intermediaries and technology platforms that use machine-learning systems, artificial intelligence, or other generative or transformative models shall establish and implement processes that:

(1) Exclude or remove CSAEM and sexually exploitative depictions of children from training, fine-tuning, or evaluation datasets, except to the limited extent expressly authorized under the safe-harbor provision for strictly necessary safety-system development, testing, validation, or operation; and

(2) Prevent the model from generating or facilitating CSAEM or the sexualization of children.

(vii) Technical Information and Cooperation. – Maintain and, upon lawful request of competent authorities, provide information reasonably necessary to understand the relevant technical features of the platform for purposes of OSAEC or CSAEM investigation or policy-making, including, as appropriate, documentation on safety features, default configurations, content-guardrail mechanisms, and other comparable technical or operational information.

(viii) Provision of Subscriber Information and Traffic Data. – Provide upon lawful request from law enforcement, competent authorities, and legislative bodies acting in aid of legislation, such subscriber or registration information and traffic data, in the covered entity's control and possession, as are specifically described in the request and relevant to the investigation of a person who:

(1) Gained or attempted to gain access to an internet site, internet asset, or internet application containing CSAEM or through which any form of OSAEC is being committed; or

(2) Committed, facilitated, or attempted to commit any OSAEC- or CSAEM-related act under this Act.

The request must particularly describe the information sought and state its relevance to the OSAEC and/or CSAEM case.

Responsible officers, employees, and other personnel who obtain access to such data pursuant to this section shall not disclose, publish, reveal, share, or use the same except as lawfully authorized and strictly necessary for investigation, prosecution, judicial proceedings, inter-agency coordination, evidence preservation, legislative inquiry in aid of legislation, or international cooperation under this Act and other applicable laws.

(ix) Risk and Child-Safety Assessment. – Conduct, document, retain, and keep updated, in a manner proportionate to the nature, size, functionality, technical architecture, and risk profile of their services, risk and child-safety assessments on how their services, systems, design, features, functionalities, user-interaction tools, recommender systems, or monetization mechanisms may be used to commit, facilitate, promote, conceal, monetize, or transmit OSAEC, CSAEM, or related technology-facilitated child sexual abuse or exploitation.

Such assessment shall likewise be conducted or updated before deploying or materially modifying any service, feature, functionality, system, policy, or other aspect of the service that may reasonably affect the risk of OSAEC, CSAEM, or related technology-facilitated child sexual abuse or exploitation.

Internet intermediaries and technology platforms shall submit the assessment, or a summary thereof, to the NCC, through the NC-COpS, when required under this Act, the implementing rules and regulations, applicable compliance codes, or a lawful directive of the NCC, subject to confidentiality, trade secret, security, data protection, and child protection safeguards.

(c) Duties of Data Transmission Industry Participants (DTIPs) and Internet Service Providers (ISPs) that only provide network connectivity. – For DTIPs and ISPs that only provide network connectivity and do not operate user-facing content or application services, compliance with this subsection shall relate to network-layer systems, designs, and procedures within their technical control, including, at a minimum:

(i) Maintaining and applying lists, feeds, hashes, digital fingerprints, or other technical identifiers issued, maintained, authorized, or recognized by competent authorities, regulators, courts, internationally recognized child-protection hotlines or clearinghouses, or reputable child-safety organizations, for blocking, restriction, preservation, reporting, or other network-layer measures under this Act, where such identifiers involve Internet addresses, domains, subdomains, URLs, websites, web pages, proxy or mirror sites, file-sharing or cloud-storage links, application or invite links, platform components, or other technically identifiable Internet assets containing CSAEM or used to commit or facilitate OSAEC;

(ii) Preserving subscriber information, traffic data, IP address logs, and other network-layer records as required under this Act, other applicable laws, or lawful orders;

(iii) Implementing lawful blocking or access-restriction orders involving identified Internet addresses, domains, subdomains, URLs, websites, web pages, proxy or mirror sites, file-sharing or cloud-storage links, application or invite links, platform components, or other technically identifiable Internet assets containing CSAEM or used to commit or facilitate OSAEC; and

(iv) The blocking or disabling of access to identified internet addresses, domains, or URLs containing CSAEM or used for OSAEC:

Provided, That the use of such identifiers shall be subject to safeguards against inaccuracy, unauthorized disclosure, and overblocking, including updating, audit, and correction procedures, as may be prescribed in the implementing rules and regulations.

Where technological developments or service changes enable a DTIP or ISP to perform functions beyond mere network connectivity, the NCC, in coordination with the appropriate regulator, may determine the additional obligations applicable to such provider under this Act, after assessment of technical capability, necessity, proportionality, privacy, cybersecurity, and child protection considerations.

(d) Duties of Device Manufacturers and Device-Environment Providers. – Device manufacturers, operating system providers, and developers of device environments for covered devices shall adopt and maintain built-in, reasonable, and proportionate technical safeguards designed to prevent, detect, filter, block, restrict, or interrupt the creation, recording, editing, storage, export, upload, transmission, or sharing of CSAEM through or within such devices, operating systems, or device environments, having due regard to the nature, functionality, and risk profile of the product.

Such safeguards may include, where technically feasible and appropriate, content guardrails, hash-matching, digital fingerprinting, warnings or interruptions, export or sharing restrictions, reporting channels, default safety configurations, and other equivalent protective measures to be further prescribed in the IRR.

Nothing in this subsection shall be construed to require generalized or indiscriminate monitoring of all user content, or to require access to user-generated content stored solely on an end-user's device beyond what is reasonably necessary to operate built-in safety features or to comply with a specific lawful request or order under applicable law.

(e) Additional Duties of Payment Service Providers and Related Financial Entities. – In addition to the duties applicable to them under paragraph (A), all PSPs and VASPs when performing payment, transfer, or settlement functions, shall:

(i) Traceability and Data-Sharing Mechanisms. – Ensure effective traceability of transactions by maintaining interoperable, auditable, and secure data-sharing mechanisms with other PSPs when a customer, account, product, channel, or transaction is identified or reasonably suspected as being connected to OSAEC or CSAEM. This mechanism should ensure that cross-platform fund flows can be traced.

Further, such mechanisms shall operate within the periods and in accordance with the technical and operational standards prescribed by the primary regulator of PSPs and VASPs, taking into account the size, nature, and risk to OSAEC or CSAEM activity of the service.

(ii) Preservation of Customer, Account, Transaction, and Related Technical Data. – Preserve, in a manner that ensures authenticity, integrity, and reliability, customer or account registration information, wallet or payment-instrument identifiers, transaction records,

beneficiary and originator information, merchant information, payment-reference or narrative fields, IP addresses, timestamps, device or access logs, and other related technical or transactional data within their possession, custody, or control that are generated, received, recorded, or maintained in the ordinary course of business in relation to customer onboarding, account activity, access events, wallet activity, payment instruments, or transactions.

Such data shall be preserved for at least the periods required under Republic Act No. 9160, otherwise known as the Anti-Money Laundering Act of 2001, as amended, its implementing rules and regulations, relevant issuances of the BSP and the Anti-Money Laundering Council (AMLC), and other applicable laws, and for such longer period as may be required by lawful request, notice, or order of a competent authority under this Act or other applicable law.

For purposes of this paragraph, related technical or transactional data may include non-content data associated with access to, use of, or transactions through the payment service, including IP addresses, timestamps, session logs, device identifiers, geolocation data where collected, routing or channel information, and similar records, to the extent maintained by the PSP or VASP in the ordinary course of business.

Nothing in this paragraph shall be construed to reduce or limit any preservation duty applicable under this Act, Republic Act No. 9160, as amended, BSP regulations, AMLC regulations, or lawful orders of competent authorities.

(iii) Access to Financial, Account, and Related Technical Information; Cooperation with Authorities. – Cooperate with competent authorities and disclose or provide access to the following, notwithstanding Republic Act Numbered 1405, 6426, and 8791:

(1) Upon lawful request of competent authorities – basic customer or account identifying information, including name, registered contact information, customer or account number, wallet or payment-instrument identifiers, account status, IP addresses, timestamps, device or access logs, session logs, routing or channel information, and other comparable technical or transactional data within their possession, custody, or control, as are specifically described in the request and reasonably necessary for identification, tracing, preservation, investigation, detection, or disruption of OSAEC- or CSAEM-related activity under this Act;

(2) Upon *subpoena* by government entities authorized to issue *subpoenas* – in addition to those mentioned in the preceding paragraph, financial documents and information reasonably necessary where there is reasonable ground to believe that transactions are related to OSAEC or CSAEM offenses, including Know-Your Customer (KYC) or Customer Due Diligence (CDD) records, customer identification documents, account opening files, and transaction records for specified periods, together with merchant or counterparty details, originator and beneficiary information, and narrative or payment-reference fields.

The good-faith processing and disclosure of information under this subsection shall constitute lawful processing under Republic Act No. 10173 and shall not hold the PSPs and VASPs civilly, criminally, or administratively liable under bank-secrecy or data-privacy laws.

Nothing in this paragraph shall be construed to limit or modify the powers of the AMLC under Republic Act No. 9160, as amended, and its IRR.

Competent authorities, legislative bodies acting in aid of legislation, and their responsible officers, employees, and other personnel who obtain access to financial documents or information pursuant to this Act, shall securely protect the same and shall not disclose, publish, reveal, share, or use such information except as lawfully authorized and strictly necessary for investigation, prosecution, judicial proceedings, regulatory or enforcement action, and legislative inquiry in aid of legislation. This prohibition shall apply even after their separation from government service.

(iv) Development of Internal Systems to Detect Risks in Transactions Potentially Involving OSAEC and CSAEM. – Develop, implement, and maintain appropriate technical and organizational systems, designs, or procedures for preventing, detecting, blocking, restricting and reporting transactions that involve the commission of OSAEC crimes as defined under this Act pursuant to BSP/AMLC issuances on the matter. These may include, but not limited to, the use of automated tools or other algorithmic or Artificial Intelligence-based classifiers, or other similar tools that may flag high-risk or abnormal financial activity.

The BSP shall likewise develop guidelines on banking compliance obligations, the development of internal systems to detect and prevent the use of PSPs and their platforms for transactions relating to OSAEC and other mechanisms that shall

pursue collective cooperation among PSPs and other financial institutions to identify suspicious financial transactions relating to OSAEC activities.

No PSP shall refuse to adopt such measures as recommended by the BSP. PSPs that refuse to adopt such measures shall be subject to administrative sanctions under Section 45 of this Act.

(v) OSAEC and CSAEM Financial Risk Assessment. – Conduct, document, retain, and periodically update, in a manner proportionate to the nature, scale, products, channels, technical architecture, and risk profile of their operations, conduct, document, retain, and periodically update risk assessments on how their accounts, products, channels, services, or systems may be used to facilitate, monetize, conceal, or transmit funds or proceeds linked to OSAEC, CSAEM, or related technology-facilitated child sexual abuse or exploitation.

Such assessment shall inform the development and periodic review of appropriate controls, typologies, red-flag indicators, transaction-monitoring measures, escalation procedures, preservation mechanisms, reporting protocols, and cooperation arrangements with competent authorities, consistent with BSP, AMLC, SEC, and other applicable regulations and issuances.

The assessment shall be updated before deploying or materially modifying any product, service, channel, onboarding process, merchant service, wallet or virtual asset feature, transaction-monitoring system, or other operational change that may materially affect the risk of OSAEC- or CSAEM-related financial activity.

(vi) Applicability of Internet Intermediary and Technology Platform Duties. – Where a PSP or VASP also qualifies as an internet intermediary or technology platform under this Act, the corresponding duties applicable to internet intermediaries and technology platforms shall also apply to them.

SEC. 28. *Additional Duties of Covered Entities with Enhanced Safeguarding Duties.* – Covered Entities with Enhanced Safeguarding Duties, as defined in Section 3 of this Act, in addition to duties prescribed in Section 27, shall:

(a) OSAEC Risk Assessments. – In addition to the risk-assessment duties under this Act, conduct, document, retain, and keep updated enhanced OSAEC and CSAEM risk assessments at least once every twelve (12) months, or at a more frequent interval as may be determined by the NCC, and before deploying or materially modifying any service, feature, functionality, system, design, product, channel, business model, policy, or other operational change that may materially affect the risk of violations of this Act.

Internet intermediaries and technology platforms shall submit the assessment, or a summary thereof, to the NCC, through the NC–COpS, when required under this Act, the implementing rules and regulations, applicable compliance codes, or a lawful directive of the NC–COpS, subject to confidentiality, trade secret, security, data protection, and child protection safeguards.

(b) Law Enforcement Portal. – Establish and maintain a secure and continuously available law enforcement portal through which competent or duly authorized Philippine authorities may submit lawful requests, notices, reports, preservation requests, subpoenas, court orders, takedown or disablement directives, and other communications authorized under this Act or other applicable laws.

The portal shall allow secure electronic submission, receipt, acknowledgement, and tracking of requests, and support the prompt handling of urgent matters involving imminent harm, ongoing abuse or exploitation, active livestreaming, or immediate preservation needs.

(c) Urgent Escalation Procedures. – Maintain internal procedures for the urgent escalation and handling of cases involving imminent harm to a child, ongoing livestreaming, active sexual extortion, active grooming or luring presenting immediate risk of abuse, rapid dissemination of child sexual abuse or exploitation materials, or other analogous circumstances requiring immediate intervention.

(d) Child Safeguarding Officer. – Designate and maintain a safeguarding officer to oversee compliance with this Act and lawful directives issued hereunder, without prejudice to any separate requirement under this Act to designate a Philippine legal representative.

(e) Transparency Reports. – Publish transparency reports at least once every six (6) months, detailing content modification practices and actions taken against OSAEC and CSAEM.

(f) Designated Philippine Legal Representative for Foreign Covered Entities with Enhanced Safeguarding Duties. – Foreign Covered Entities with Enhanced Safeguarding Duties that offer, provide, or make their platforms services, products, or functionalities available in or into the Philippines, whether or not they have a physical presence in the country, shall designate a Philippine legal representative within six (6) months from notice or publication of their designation, or within such shorter period as the NC–COpS may prescribe in urgent or meritorious cases involving imminent harm, ongoing abuse or exploitation, or repeated non-compliance. Any shortened period shall be based on a written determination stating the urgency, risk, repeated non-compliance, or operational necessity relied upon, and shall be subject to review under the rules prescribed in the IRR.

The legal representative shall be a resident of the Philippines or a juridical person organized or duly licensed to do business in the Philippines, duly authorized to receive and respond to notices, orders, directives, preservation requests, subpoenas, petitions, court processes, service of process, and other lawful communications under this Act. The designation shall be registered with the NC–COpS, which shall maintain the official registry and provide access thereto to competent authorities as may be appropriate.

The implementing rules and regulations shall prescribe the form, qualifications, authority, duties, contact details, registration, updating, and other requirements for designated legal representatives.

SEC. 29. ***Duties of Public Wi-Fi Providers, Internet Hotspots, Cafés, and Kiosks.*** –

(a) Duties. – All public Wi-Fi providers, internet hotspots, internet cafés, kiosks, and similar establishments offering public access to the internet shall:

(1) Prohibit the Use of Premises and Facilities for OSAEC and CSAEM. – Prohibit and take reasonable measures to prevent the use of their premises, facilities, devices, equipment, internet access, networks, or services for the commission, facilitation, livestreaming, production, distribution, possession, viewing, storage, transmission, or attempted commission of OSAEC, CSAEM, or any violation of this Act;

(2) Notification to Law Enforcement. – Notify law enforcement authorities within twenty-four (24) hours from obtaining facts and circumstances reasonably indicating that any violation of this Act is being committed, facilitated, or attempted within their premises or through the use of their facilities, devices, equipment, internet access, networks, or services:

Provided, That where the act or omission is committed within the premises of such public Wi-Fi provider, internet hotspot, café, kiosk, or similar establishment, the person in charge thereof shall be deemed to have prima facie knowledge of such act or omission, unless the contrary is shown;

(3) Awareness and Hotline Signages. – Promote awareness against OSAEC and CSAEM through clear, visible, and child-sensitive signages in English, Filipino, or, where appropriate, the local language or dialect, stating that the use of the premises, facilities, devices, internet access, networks, or services for OSAEC or CSAEM is strictly prohibited, and displaying relevant local and national reporting hotlines within the premises.

(b) Local Government Units Compliance and Enforcement. – Local Government Units (LGUs) shall ensure compliance with this section within their respective jurisdictions by integrating the requirements herein into their business permitting, inspection, child protection, and local reporting mechanisms. For this purpose, LGUs shall:

(1) Integrate compliance in business permitting. – Condition the issuance and renewal of business permits, licenses, clearances, or similar local authorizations for public Wi-Fi providers, internet hotspots, internet cafés, kiosks, and similar establishments offering public internet access on proof of compliance with this section;

(2) Require and verify signages and reporting information. – Require and verify the posting of clear, visible, and child-sensitive signages in English, Filipino, or, where appropriate, the local language or dialect, stating that the use of the premises, facilities, devices, internet access, networks, or services for OSAEC, CSAEM, or any violation of this Act is strictly prohibited and punishable by law, and indicating local and national reporting hotlines;

(3) Conduct inspections and compliance monitoring. – Conduct regular and spot inspections to verify compliance with this subsection, including the posting of required signages and hotlines, the adoption of reasonable preventive measures, and, where applicable, the presence and proper configuration of blocking or filtering software or other child-protective safeguards;

(4) Designate a child-protection focal office or officer. – Designate a child-protection focal office or officer responsible for receiving reports, in accordance with existing guidelines and protocols;

(5) Provide orientation and compliance materials. – Provide or facilitate orientation, advisories, and compliance materials for operators, owners, managers, and staff of covered establishments, based on standards, templates, or guidance issued by the NCC; and

(6) Enforce compliance through administrative sanctions. – After due notice and hearing, enforce compliance with this subsection through the imposition of administrative sanctions authorized under this Act, its IRR, and applicable local ordinances, including warning, compliance order, fine, suspension, non-renewal, or revocation of business permit or license, closure order, or other appropriate administrative sanctions, without prejudice to criminal, civil, administrative, or other liability under this Act and other laws.

SEC. 30. ***Duties of Learning Institutions and Supplementary Learning and Youth Activity Centers.*** – Learning Institutions and Supplementary Learning and Youth Activity Centers, as defined in Section 3 of this Act shall:

(a) Common Duties of Learning Institutions and Supplementary Learning and Youth Activity Centers:

(1) Child Protection Structures and Policies. – Strengthen institutional policies, codes of conduct and functional child protection mechanisms, including: (1) a Child Protection Committee or equivalent structure; and (2) a designated focal person trained in identification, response, and referral of OSAEC or CSAEM cases; and provide safe and non-stigmatizing environments for learners who are victims or at risk, and facilitate access to appropriate support services and referrals.

The policy shall be made known to personnel, volunteers, learners, and parents/guardians in a manner appropriate to their age and capacity.

(2) Absolute Protection and Non-Penalization of Victim-Learners. – Learners who are victims of OSAEC or CSAEM shall be treated as victim-survivors and shall not be penalized or subjected to disciplinary action solely on account of their victimization. This protection shall include cases involving self-generated or first-person–produced CSAEM depicting the learner-victim, provided that no other child is involved, depicted, exploited, coerced, or victimized.

(3) Mandatory Reporting and Referral. – Heads, owners, managers, personnel or volunteers who know or reasonably suspect that a learner is a victim of, or at risk of, OSAEC or CSAEM, shall, without undue delay and in no case later than twenty-four (24) hours from knowledge or reasonable suspicion:

(i) Report the matter to the appropriate law enforcement agencies and/or local Social Welfare and Development Office (SWDO), following existing referral pathways; and

(ii) Document the incident, following existing referral pathways, and preserve relevant information in a manner consistent with applicable laws and guidelines.

They shall not conduct unauthorized investigations that may compromise the integrity of evidence or child safety.

(4) Capacity Building. – Ensure that teaching and other relevant personnel and volunteers receive periodic training on identifying, reporting, and responding to OSAEC and CSAEM, including trauma-informed handling of disclosures and the confidentiality, privacy, and safe handling of child-victim information, reports, and related records.

(5) Safe and Secure Digital Environments. – Ensure that school or center-managed or facilitated digital environments are safe for learners. They shall implement reasonable and proportionate safeguards to prevent the use of school connectivity, systems, devices, or platforms for OSAEC or CSAEM, consistent with national policies on connectivity and open access, including the Free Internet Access in Public Places Act, and relevant standards issued by the DICT, Department of Education (DepEd), Commission on Higher Education (CHED), and Technical Education and Skills Development Authority (TESDA) and LGUs.

(6) Coordination with Competent Authorities. – Cooperate and coordinate with competent authorities in the prevention, detection, reporting, referral, rescue, investigation, and handling of OSAEC and CSAEM cases. Upon lawful request, they shall provide relevant information, records, documents, or assistance within their custody, possession, or control, as may be necessary for victim identification, child protection intervention, rescue operations, case build-up, investigation, prosecution, or referral of OSAEC and CSAEM cases.

The good-faith disclosure or sharing of information pursuant to a lawful request under this Act, and for the purposes stated herein, shall not constitute a violation of data privacy laws, confidentiality rules, school policies, or contractual obligations: *Provided,* That such disclosure or sharing is limited to information relevant and necessary for the stated purpose, properly documented, and made only to competent authorities or other duly authorized persons.

(b) Additional Duty of Learning Institutions:

In addition to the foregoing common duties prescribed in paragraph (a), learning institutions shall integrate age-appropriate online safety and anti-OSAEC/CSAEM education into relevant curricula, advisories, orientation programs, co-curricular activities, and other learner development programs, as may be prescribed by the DepEd, CHED, and TESDA.

For this purpose, DepEd, CHED, and TESDA shall develop, adopt, and periodically update the necessary continuing, age-progressive, and developmentally appropriate curricula, modules, standards, advisories, and learning materials for online safety and the prevention of OSAEC and CSAEM, for implementation by learning institutions under their respective jurisdictions.

Such education shall be delivered on a regular and recurring basis, in accordance with the minimum content, standards, and frequencies to be prescribed in the implementing rules and regulations.

(c) Monitoring, Compliance, and Implementing Rules:

(1) Monitoring - DepEd, CHED, and TESDA shall monitor compliance of Learning Institutions with their duties under this Section and shall enforce compliance through the imposition of administrative sanctions authorized under this Act, its IRR, or other appropriate administrative sanctions, without prejudice to criminal, civil, administrative, or other liability under this Act and other laws.

(2) Compliance - CHED, DepEd, and TESDA shall also ensure compliance with this subsection by integrating the duties and responsibilities herein into their business permitting, accreditation, licensing, and clearances for learning institutions and supplementary youth activity centers. For this purpose, CHED, DepEd, and TESDA shall:

(i) Condition the issuance and renewal of business permits, licenses, clearances, accreditation, or similar local authorizations for learning institutions and supplementary youth activity centers on proof of compliance with this section;

(ii) Conduct regular and spot inspections to verify compliance with this subsection, including the existence of child-protection policies, designated focal persons, training programs, reporting and referral pathways, and basic safeguards in online and offline environments.

LGUs shall monitor compliance of Supplementary Learning and Youth Activity Centers with their duties under this section. LGUs may, consistent with this Act and its IRR;

(iii) Condition the issuance and renewal of business permits or authorizations for private youth activity centers on minimum compliance with this section;

(iv) Conduct regular or spot inspections to verify the existence of child-protection policies, focal persons, and basic safeguards; and

(v) Impose administrative sanctions authorized under this Act, its IRR, or other appropriate administrative sanctions, without prejudice to criminal, civil, administrative, or other liability under this Act and other laws.

(3) Implementing Rules and Regulations - The DepEd, CHED, TESDA, and DILG, in coordination with the NC–COpS and other relevant agencies, shall issue the implementing rules and regulations for this section, including differentiated and proportionate requirements based on the size, capacity, and context of learning institutions.

SEC. 31. ***Extraterritorial Application to Covered Entities.*** – This Act shall apply to any covered entity, whether based in the Philippines or abroad, that makes its platforms, services, products, or functionalities available in or into the Philippines, whether or not it has physical presence, incorporation, registration, personnel, assets, servers, or facilities in the country.

SEC. 32. ***Service of Processes; Legal Representative; Substitute and Electronic Service.*** – In case of non-designation, unavailability, refusal, or failure of the legal representative or any authorized point-of-contact of a domestic or foreign covered entity to receive or act on valid service, service may be made by any reasonable electronic or substituted means reasonably calculated to give notice to the covered foreign entity, including through its published point of contact, compliance or law enforcement request channel, abuse-reporting portal, official email address, website or application contact mechanism, domestic affiliate, agent, contractor, or other known representative, or such other means as may be prescribed in the IRR. Proof of transmission or attempted transmission through such means shall be sufficient basis to proceed under this Act, without prejudice to the right of the respondent to appear, comply, seek modification, or contest the process in accordance with due process.

CHAPTER V
INSTITUTIONAL FRAMEWORKS

SEC. 33. ***The National Council for Child Online Safety and Protection.*** – There is hereby created the National Council for Child Online Safety and Protection, hereinafter referred to as the NCC, as an attached agency of the Department of Justice.

The NCC shall serve as the national inter-agency coordinating, policy-making, regulatory, compliance-monitoring, and strategic direction-setting body for the prevention, detection, reporting, disruption, investigation support, prosecution support, protection, recovery, reintegration, and overall national response to OSAEC, CSAEM, and all forms of technology-facilitated child sexual abuse or exploitation.

For this purpose, the NCC shall oversee the implementation of this Act, including the harmonization of national and local policies, standards, protocols, referral mechanisms, compliance systems, and inter-agency actions, to ensure a coordinated, victim-centered, child-sensitive, trauma-informed, survivor-informed, rights-based, and whole-of-nation response against OSAEC and CSAEM, and all forms of technology-facilitated child sexual abuse or exploitation.

SEC. 34. ***Composition of the NCC.*** – The NCC shall be chaired by the Secretary of the Department of Justice (DOJ) and co-chaired by the Secretary of the Department of Social Welfare and Development (DSWD).

The Secretary of the Department of Information and Communications Technology (DICT) shall serve as Vice-Chairperson for Digital Safety and Technology, and the Secretary of the Department of the Interior and Local Government (DILG) shall serve as Vice-Chairperson for Local Implementation and LGU Compliance.

The NCC shall be composed of the following member-agencies and offices:

(1) Department of Justice, as Chairperson;
(2) Department of Social Welfare and Development, as Co-Chairperson;
(3) Department of Information and Communications Technology, as Vice-Chairperson for Digital Safety and Technology;
(4) Department of the Interior and Local Government, as Vice-Chairperson for Local Implementation and LGU Compliance;
(5) Department of Education;
(6) Department of Health;
(7) Department of Foreign Affairs;
(8) Department of Labor and Employment;
(9) Department of Tourism;

(10) Department of Trade and Industry;
(11) Office of the Chief Minister, Bangsamoro Autonomous Region in Muslim Mindanao;
(12) National Authority for Child Care;
(13) National Commission on Indigenous Peoples;
(14) National Youth Commission;
(15) Inter-Agency Council Against Trafficking (IACAT);
(16) National Council on Disability Affairs;
(17) Council for the Welfare of Children;
(18) Philippine National Police;
(19) National Bureau of Investigation;
(20) DOJ-Office of Cybercrime;
(21) Philippine Center for Transnational Crime;
(22) Philippine Information Agency;
(23) Presidential Office for Child Protection;
(24) National Prosecution Service;
(25) Bureau of Immigration;
(26) Anti-Money Laundering Council;
(27) Bangko Sentral ng Pilipinas;
(28) National Telecommunications Commission;
(29) National Privacy Commission;
(30) Cybercrime Investigation and Coordinating Center;
(31) Commission on Human Rights;
(32) Movie and Television Review and Classification Board;
(33) Representative, Child Rights Organizations;
(34) Representative, Child Online Safety Organizations;
(35) Representative, Survivors Groups; and
(36) Such other agencies, offices, or instrumentalities as may be admitted by the NCC.

The heads of member-agencies and offices may designate permanent and alternate representatives who shall have a rank not lower than Assistant Secretary or its equivalent.

The NCC may invite or designate other government entities, relevant private sector groups or institutions, academe, civil society organizations, development partners, and other stakeholders as members of standing committees, technical working groups, or advisory groups, or as observers or resource persons, as may be necessary for the implementation of this Act.

The NCC shall likewise be a member of the IACAT.

SEC. 35. *Standing Committees and Functional Clusters.* – The NCC may establish standing committees, functional clusters, technical working groups, or other coordination mechanisms necessary for the effective implementation of this Act.

Unless otherwise determined by the NCC, the following functional clusters shall be established:

(1) Prevention and Advocacy;
(2) Protection and Response;
(3) Prosecution, Enforcement, and Compliance; and
(4) Partnership and Networking.

The lead and co-lead agencies shall coordinate the formulation, implementation, monitoring, and reporting of policies, programs, standards, protocols, and measures within their respective clusters, subject to the strategic direction, policies, and decisions of the NCC. The NCC shall designate appropriate lead and co-lead agencies from among its member-agencies and offices, taking into account their respective mandates, expertise, and implementation responsibilities.

The NCC may revise, consolidate, expand, discontinue, or create additional clusters, committees, or technical working groups as may be necessary.

SEC. 36. *Powers and Functions of the NCC.* – The NCC shall oversee the implementation of this Act, and shall have the following powers and functions:

(a) Policy and strategy. – Formulate, adopt, harmonize, and periodically update national policies, strategies, standards, protocols, and guidelines on OSAEC, CSAEM, and other technology-facilitated forms of child sexual abuse or exploitation;

(b) Coordination. – Coordinate and harmonize the programs, referral pathways, reporting mechanisms, data systems, and operational arrangements of member-agencies, local government units, covered entities, and other stakeholders;

(c) Regulation and compliance. – Monitor compliance with this Act; require reports and compliance submissions; issue rules, guidelines, circulars, advisories, standards, and directives; conduct or coordinate compliance assessments; and recommend or impose administrative measures or sanctions as authorized by this Act, subject to due process;

(d) Reporting, referral, triage, and clearinghouse coordination. – Establish policy direction, standards, and strategic oversight for the national reporting, referral, and triage system for OSAEC and CSAEM reports and referrals, including foreign referrals, cybertipline reports, and reports from foreign hotlines,

clearinghouses, international organizations, and analogous entities. The system shall be operationalized through the NC–COpS, the Philippine Internet Crimes Against Children Center (PICACC), and other competent agencies in accordance with their respective mandates and approved referral protocols. This is without prejudice to the functions of the designated central authority or competent authority in matters requiring mutual legal assistance, extradition, formal international cooperation, or other treaty-based or law-based processes;

(e) Data, research, and monitoring. – Establish policy direction, standards, and oversight for a secure, child-sensitive, and interoperable national data, research, monitoring, analytics, and case-tracking system on OSAEC and CSAEM, covering reports, referrals, cases, services, compliance, programs, trends, and other information necessary to implement this Act;

(f) Victim protection and justice-sector coordination. – Provide policy direction, standards, and inter-agency coordination for victim identification, rescue, referral, protection, recovery, reintegration, aftercare, and access to justice in a child-sensitive, trauma-informed, survivor-centered, and rights-based manner, ensuring the safety, dignity, privacy, best interests, and continuity of care of child victims;

(g) Prevention, education, and capacity-building. – Develop, coordinate, and monitor prevention, awareness, education, communications, training, and technical-assistance programs for competent authorities, LGUs, covered entities, children, families, communities, and other stakeholders;

(h) Participation and partnerships. – Establish safe, ethical, meaningful, and trauma-informed mechanisms for child, youth, and survivor participation, and build partnerships with government, civil society, academe, private sector, development partners, foreign governments, international organizations, and other stakeholders;

(i) Internal governance. – Adopt internal rules, resolutions, issuances, organizational arrangements, strategic plans, work plans, and performance targets necessary for the effective performance of its functions;

(j) Reports and recommendations. – Require periodic reports from the NC–COpS, member-agencies, local government units, covered entities, and other relevant stakeholders, and submit reports and recommendations to the President, Congress, and appropriate agencies; and

(k) Residual authority. – Perform such other powers and functions as may be necessary or incidental to the effective implementation of this Act.

SEC. 37. *Meetings and Quorum of the NCC.* –

(a) Regular Council Meetings - The NCC shall hold regular coordination meetings at least once every quarter, upon the call of the Chairperson, the Co-Chairperson, or their duly authorized representatives.

(b) Special Meetings - As the need arises, special meetings may be convened by the Chairperson, Co-Chairperson, Vice-Chairperson or their authorized representative, or upon the written request of at least one-third (1/3) of the member-agencies or offices.

(c) Presiding Officer - Meetings shall be presided over by the Chairperson or the Chairperson's duly designated representative. In their absence, the Co-Chairperson or the Co-Chairperson's duly designated representative shall preside. In the absence of both, a Vice-Chairperson designated by the Chairperson, or determined in accordance with the internal rules of the NCC, may preside.

(d) Quorum - A majority of the member-agencies and offices of the NCC shall constitute a quorum. For purposes of determining quorum and voting, each member-agency or office shall have one (1) vote, to be cast by its head or duly authorized representative. All matters requiring Council approval shall be decided by a majority vote of the members present, there being a quorum, unless a higher vote is required by this Act or its implementing rules and regulations.

(e) Modality - Meetings may be conducted in person, through videoconferencing, other secure electronic means, or a hybrid format. Participation through such means shall be deemed attendance for purposes of quorum and voting.

SEC. 38. *The National Child-Safety Command and Operations Service (NC–COpS).* – There is hereby created a National Child-Safety Command and Operations Service, hereinafter referred to as the NC-COpS which shall serve as the permanent operating arm of the NCC, providing technical, operational, compliance, data, referral coordination, and administrative and secretariat support.

The NC-COpS shall support, facilitate, coordinate, and monitor the implementation of the policies, resolutions, directives, standards, protocols, programs, and decisions of the NCC, in coordination with member-agencies, local government units, sectoral regulators, law enforcement agencies, prosecution offices, social welfare authorities, covered entities, and other relevant agencies and stakeholders.

The NC-COpS shall be provided with adequate personnel, resources, internal support units, and administrative, technical, financial, legal, data, compliance,

referral, and operational support mechanisms necessary for the effective performance of its functions, subject to the approved organizational structure, staffing pattern and applicable government rules and regulations.

The NC-COpS shall be headed by an Executive Director, who shall be appointed in accordance with law and shall have the rank, qualifications, tenure, and emoluments as may be provided in this Act, its implementing rules and regulations, and other applicable laws.

SEC. 39. ***Functions of the National Child-Safety Command and Operations Service (NC-CoPS).*** – The NC-COpS shall have the following functions:

(a) Secretariat support. – Provide secretariat support to the NCC and its standing committees, functional clusters, technical working groups, and advisory groups, including the preparation of agenda, minutes, resolutions, reports, records, notices, meeting materials, documentation, and follow-through on decisions, directives, and action points;

(b) Implementation support. – Support, facilitate, coordinate, and monitor the implementation of this Act, its IRR, and related policies, resolutions, directives, standards, protocols, programs, and work plans by member-agencies, local government units, sectoral regulators, covered entities, and other relevant stakeholders;

(c) Reporting, referral, triage, and clearinghouse coordination. – Operate or coordinate the national reporting, referral, and triage system for OSAEC, CSAEM, and related technology-facilitated child sexual abuse or exploitation cases, reports, and referrals, and serve as the designated operational point-of-contact for foreign hotlines, clearinghouses, reporting mechanisms, international organizations, covered entities, and analogous non-law-enforcement sources transmitting OSAEC, CSAEM, or related technology-facilitated child sexual abuse or exploitation reports or referrals with a Philippine nexus, without prejudice to the PICACC provisions of this Act;

(d) Policy and standards support. – Assist the NCC in drafting rules, regulations, guidelines, circulars, advisories, templates, reporting formats, compliance standards, risk indicators, protocols, and other issuances necessary to implement this Act;

(e) Regulatory and compliance support. – Support the exercise of the regulatory authority of the Secretary of Justice and the NCC under this Act, including compliance monitoring, lawful information-gathering, preservation requests, technical assessments, and preparation of findings,

recommendations, draft directives, and proposed administrative actions or sanctions;

(f) Law enforcement and prosecution support. – Assist law enforcement agencies, prosecutors, and other competent authorities in victim identification, referral verification, report triage, de-confliction, case build-up, investigation, prosecution, digital evidence preservation, financial tracing, and forensic examination or analysis. For purposes of referral verification, victim identification, case build-up, evidence preservation, and support to investigations and prosecutions, the NC–COpS may, through the Executive Director or duly authorized officers, issue preservation requests, subpoenas, or production orders; conduct or assist in digital forensic examination or analysis; and apply for or support applications for cybercrime warrants, court orders, or other judicial processes, in coordination with competent authorities, subject to applicable safeguards;

(g) Data, research, and monitoring systems. – Establish, maintain, operate, or support the national data, research, monitoring, analytics, referral, compliance, and case-tracking systems on OSAEC and CSAEM;

(h) Data Fusion Center. – Establish, maintain, or operate a secure, child-sensitive, and interoperable Data Fusion Center for the lawful integration, deconfliction, analysis, and visualization of OSAEC and CSAEM reports, referrals, case information, compliance data, financial indicators, foreign referral data, cybertipline reports, victim and offender indicators, and other relevant datasets, in support of victim identification, referral triage, case build-up, trend and threat analysis, policy formulation, compliance monitoring, and inter-agency coordination, subject to data protection, confidentiality, cybersecurity, access-control, audit-trail, and child protection safeguards;

(i) Victim protection coordination. – Coordinate with competent agencies and service providers for victim identification, rescue coordination, referral, emergency protection, psychosocial support, legal assistance, recovery, reintegration, and aftercare;

(j) Capacity-building and technical assistance. – Develop, coordinate, facilitate, or support capacity-building programs, including through technical or resource assistance, and provide guidance, tools, and templates for member-agencies, local government units, covered entities, and other relevant stakeholders. For this purpose, the Service may establish or designate, on a phased and needs-based basis, appropriate training and capacity-building center or mechanisms, subject to the approved

organizational structure and staffing pattern, availability of appropriations, and applicable government rules;

(k) Monitoring, evaluation, and reporting. – Prepare and submit to the NCC regular operational, compliance, data, monitoring, and performance reports, including recommendations for policy, regulatory, operational, budgetary, administrative, or legislative action;

(l) Confidentiality and data protection. – Ensure the lawful, secure, child-sensitive, and confidential processing of child-victim, survivor, case-related, referral, compliance, and operational information handled by the Service; and

(m) Other functions. – Perform such other functions as may be assigned by the NCC, the Chairperson, the Co-Chairperson, or as may be necessary to implement this Act.

SEC. 40. ***Supervision and Accountability.*** – The NC-COpS shall be under the supervision of the NCC, through the Chairperson, and shall operate subject to the policies, resolutions, directives, and decisions of the Council.

SEC. 41. ***Executive Director and Deputy Executive Directors of the NC-COpS.*** – The NC-COpS shall be headed by an Executive Director, who shall be the chief operating and administrative officer thereof. The Executive Director shall have the same rank and privileges as that of an Undersecretary.

The Executive Director shall:

(a) Possess and demonstrate substantial knowledge, training, and experience in Anti-OSAEC and CSAEM work; and
(b) Have at least ten (10) years experience in any of the following fields: law, prosecution, law enforcement, ICT, cybersecurity, social work, child protection, or other related fields relevant to the implementation of this Act.

The Executive Director shall be under the supervision of the NCC, through the Chairperson, and shall be responsible for the day-to-day administration, management, and operations of the NC-CoPS, including the supervision of its personnel, resources, records, systems, property, and internal support mechanisms.

The Executive Director shall have the following powers and functions:

(a) Coordinate, monitor, and ensure follow-through on the policies, resolutions, directives, standards, protocols, programs, work plans, and decisions of the NCC;

(b) Direct and supervise the operations of the NC-COpS, including its technical, operational, compliance, data, referral coordination, administrative, financial, legal, capacity-building, and regional coordination functions;

(c) Submit to the NCC regular operational, compliance, data, monitoring, and performance reports, including recommendations for policy, regulatory, operational, budgetary, administrative, or legislative action;

(d) Coordinate with member-agencies, local government units, sectoral regulators, law enforcement agencies, prosecution offices, courts when appropriate, social welfare authorities, covered entities, foreign and international partners, civil society organizations, and other stakeholders for the effective implementation of this Act;

(e) Exercise or supervise the exercise of such operational, compliance, referral, data, preservation, subpoena, production, technical, forensic, and case-support functions as may be authorized under this Act, delegated by the NCC or the Chairperson, or provided in the IRR, subject to applicable safeguards;

(f) Manage the national reporting, referral, triage, monitoring, data, research, analytics, compliance, and case-tracking systems operated or supported by the NC-COpS;

(g) Recommend to the NCC the creation, consolidation, or modification of internal units, regional coordination mechanisms, technical working groups, task forces, protocols, standards, tools, templates, and capacity-building mechanisms necessary for the effective performance of the NC-COpS' functions;

(h) Represent the NC-COpS in inter-agency, domestic, foreign, and international coordination mechanisms, subject to the authority of the NCC, the Chairperson, and applicable laws on foreign affairs, mutual legal assistance, and international cooperation;

(i) Issue such internal guidelines, memoranda, and standard operating procedures as may be necessary for the efficient and coordinated performance of the NC-COpS's functions under this Act; and

(j) Perform such other functions as may be assigned by the NCC, the Chairperson, or as may be necessary to implement this Act.

The Executive Director shall be assisted by three (3) Deputy Executive Directors, each holding the same rank and privileges as that of an Assistant Secretary.

The Deputy Executive Director shall:

(a) Possess and demonstrate substantial knowledge, training, and experience in Anti-OSAEC and CSAEM work; and

(b) Have at least five (5) years experience in any of the following fields: law, prosecution, law enforcement, ICT, cybersecurity, social work, child protection, or other related fields relevant to the implementation of this Act.

The specific areas of responsibility of the Deputy Executive Director shall be defined in the IRR.

The Executive Director and Deputy Executive Directors shall be appointed by the President, upon the recommendation of the NCC.

SEC. 42. *Regional Presence and Coordination Support.* – The NC–COpS may, on a phased and needs-based basis, establish regional coordination offices, desks, focal units, or other appropriate regional mechanisms to support the implementation of this Act, subject to the approved organizational structure and staffing pattern, availability of appropriations, and applicable government rules and regulations.

The regional presence of the NC–COpS shall, as appropriate:

(a) Serve as a regional coordination mechanism for the implementation of NCC policies, programs, standards, referral pathways, data systems, and compliance support activities;

(b) Coordinate with regional and local inter-agency mechanisms, local government units, task forces, law enforcement agencies, prosecutors, social welfare and child protection authorities, learning institutions, and other competent authorities in the prevention, referral, investigation support, prosecution support, protection, recovery, reintegration, and aftercare of OSAEC and CSAEM cases;

(c) Support regional data collection, monitoring, reporting, capacity-building, technical assistance, and compliance-related activities, in accordance with standards and protocols approved by the NCC; and

(d) Perform such other functions as may be assigned by the NCC or the Executive Director, consistent with this Act.

SEC. 43. *Local Governments.* – Local governments shall pass an ordinance to localize efforts against OSAEC and CSAEM, take into account local

culture and norms, institutionalize community-based initiatives that address OSAEC and CSAEM at the barangay level, establish OSAEC and CSAEM prevention programs that aim to educate families against OSAEC and CSAEM, and provide a holistic local program for rehabilitation and reintegration under the local social welfare and development office including support and protection for victims and survivors.

LGUs shall allocate the necessary resources and budgetary support for the establishment and operation of LGU-based Child Advocacy Centers and other similar centers relating to the immediate care of rescued victims, in order to provide integrated, multi-disciplinary, and survivor-centered assistance, and the necessary resources and budgetary support to programs defined in this Act relevant to their powers and functions.

SEC. 44. ***The Philippine Internet Crimes Against Children Center (PICACC).***

(a) Establishment and Nature. – There is hereby institutionalized a Philippine Internet Crimes Against Children Center (PICACC) as a permanent inter-agency law enforcement body for OSAEC and CSAEM cases with a foreign nexus. The PICACC shall serve as the national hub for police-to-police coordination, operational deconfliction, intelligence and evidence sharing, joint and parallel investigations, and coordinated law enforcement operations involving foreign-nexus OSAEC and CSAEM cases. Subject to available resources and as may be provided in the IRR, Regional PICACC nodes may be established to enhance coverage and coordination.

(b) Foreign Nexus. – For purposes of this Act, "foreign nexus" exists where any material element of an OSAEC/CSAEM case indicates a cross-border connection, as evidenced by any of the following circumstances whether occurring singly or in combination:

(1) a suspect or a possible victim is located outside the Philippines;

(2) the conduct involves cross-border transmission, payment, or facilitation; or

(3) the referral or tip originates from a foreign law enforcement agency. The IRR shall further elaborate indicators and minimum screening steps.

(c) Composition and Operational Co-Leads. – The PICACC shall be operationally co-led by the PNP-Women and Children Protection Center (PNP-WCPC) and the NBI-Human Trafficking Division (NBI-HTRAD), or their functional successors. Other government agencies or offices mandated to investigate, prosecute, support, or coordinate OSAEC and CSAEM cases may participate as members,

observers, or resource agencies, as may be provided in the IRR, PICACC protocols, or applicable inter-agency arrangements.

(d) Funding and Logistical Support. – The PICACC shall draw its budgetary and administrative support from the appropriations of participating agencies, including a dedicated budget allocation for PICACC within the appropriations of the NCC, as well as from grants, donations, and technical assistance from development partners, and other lawful sources, subject to existing budgeting, procurement, and auditing rules.

The NCC may provide financial, logistical, technical, data, referral-monitoring, secretariat, and coordination support to PICACC, including through the NC–COpS. Nothing in this section shall be construed to confer operational command, case-selection authority, or directive control upon the NCC or the NC–COpS over the PNP, NBI, PICACC, or any participating law enforcement or investigative body

(e) Core Functions. – Within the scope of their lawful powers, the PICACC shall:

(i) Receive, docket, triage and deconflict foreign-nexus OSAEC/CSAEM referrals and leads;

(ii) Establish and maintain a structured, timely, and reciprocal information-sharing of relevant operational intelligence and updates among member-agencies in foreign-nexus OSAEC/CSAEM cases, subject to applicable secrecy, confidentiality, and data-privacy laws;

(iii) Facilitate or coordinate inter-agency investigations and operations in foreign-nexus OSAEC/CSAEM cases;

(iv) Support member-agencies with open-source intelligence, data analysis, and, where lawfully tasked, digital forensic examination and related technical services; and

(v) Generate operational statistics, threat assessments, and performance metrics to inform national policy, reporting obligations, and capacity-building priorities under this Act and related laws.

(f) Foreign Law Enforcement and Technical Partners. – Consistent with applicable international instruments, memoranda of understanding, and Philippine law, the PICACC may host or coordinate with foreign law enforcement agencies and international or non-government technical partners as liaison or technical partners for purposes of information exchange, capacity building, and

coordinated action against OSAEC/CSAEM. Such partners, however, shall have no command or operational authority over the PICACC.

(g) Reporting and Coordination with NCC. – For purposes of policy formulation, capacity-building, and performance monitoring, the PICACC shall submit to the NC–COpS periodic consolidated reports on its operations, including at a minimum:

(1) The number and basic typology of foreign-nexus OSAEC and CSAEM referrals received, triaged, and acted upon;

(2) Summary statistics on operations conducted, children safeguarded, and offenders arrested or charged;

(3) Emerging trends, threats, and operational gaps identified; and

(4) Names of reported individuals that can be included in the blacklisted alien registry.

Such reports shall contain non-operational or appropriately sanitized information, unless disclosure of case-specific or operational information is authorized by law, approved protocols, or the concerned law enforcement agency.

(h) Implementing Rules and Protocols. – The IRR, PICACC protocols, and inter-agency agreements shall prescribe the detailed procedures, safeguards, and modalities for PICACC operations, including membership and observer status; intake, triage, prioritization, deconfliction, referral, and assignment of foreign-nexus referrals; information-sharing and data fields; coordination with foreign law enforcement agencies and technical partners; confidentiality, data protection, cybersecurity, chain-of-custody, and evidence-handling safeguards; reporting to the NCC; registry-related coordination; regional nodes or coordination mechanisms; and the harmonization of existing and future memoranda of understanding, donor-supported projects, equipment, personnel details, facilities, and operational arrangements.

(i) Transitory Provision. – Existing structures of the PICACC, memoranda of understanding, facilities, donor-supported projects, equipment, personnel details, and ongoing investigations as of the effectivity of this Act are hereby recognized and shall be harmonized under this section and its IRR. Pending the promulgation of the IRR, the existing structure, memoranda of understanding, and ongoing operations of the PICACC shall continue without interruption and shall be deemed consistent with this Act.

CHAPTER VI
Regulatory Authority and Administrative Enforcement

SEC. 45. ***Regulatory Authority, Compliance Measures, and Administrative Sanctions.*** – The exercise of regulatory authority under this section shall be governed by the following rules:

(a) Sectoral Regulators. – Concerned regulators shall exercise regulatory authority over covered entities within their respective mandates or jurisdiction.

(b) Regulatory Authority of the Department of Justice. – The Secretary of Justice, as Chairperson of the NCC, or his or her duly authorized representative or designated office, and with the technical and operational support of the NC–COpS, shall exercise the regulatory authority specifically granted under this section over covered entities that are not under the regulatory or supervisory authority of any other government entity or sectoral regulator.

(c) Coordination Among Regulators. – The concerned regulators and competent authorities shall coordinate in the imposition and implementation of administrative measures and sanctions under this Act, especially where the respondent, the implementing entity, and the required measure fall under different mandates or jurisdictions. The implementing rules and regulations shall prescribe the procedures for referral, endorsement, joint action, information-sharing, service of orders, implementation reporting, post-issuance review, and resolution of overlapping or conflicting authority.

Without prejudice to criminal, civil, or other administrative liability under this Act and other applicable laws, the concerned regulator or competent authority may impose, recommend, refer, or coordinate, as appropriate, the following administrative measures or sanctions against any covered entity found to have violated this Act, its IRR, or lawful orders, compliance codes, or directives issued thereunder, subject to due process:

(a) Cease-and-Desist Order. – Issue a Cease-and-Desist order directing the respondent to immediately stop specified acts or omissions in violation of this Act, and to submit, within a reasonable period, a written report and supporting documentation demonstrating compliance.

(b) Compliance Orders. – Issue a written compliance order requiring a respondent covered entity to undertake specified corrective, preventive, or remedial actions to achieve, restore, or maintain compliance with this Act, its IRR, or lawful directives issued thereunder, including, as may be applicable:

(1) Correction of deficiencies in reporting channels, age assurance, notification, preservation, non-notification, point-of-contact, execution records, risk assessment, safety-by-design, notice-and-action, takedown, blocking, delisting, restriction, or other compliance obligations;

(2) Implementation or improvement of child-protection, risk-mitigation, technical, organizational, financial-monitoring, data-protection, or other safeguards required under this Act or its IRR;

(3) Submission of compliance reports, audit logs, risk assessments, mitigation reports, preservation records, execution records, transparency reports, or other relevant documentation;

(4) Designation, update, or empowerment of a safeguarding officer, compliance officer, legal representative, single electronic point of contact, or other responsible officer required under this Act and its IRR; and

(5) Such other necessary and proportionate remedial action as may be required under this Act.

(c) Removal, Takedown, Disablement, Restriction, or Blocking Orders. – Issue written orders directing a covered entity to remove, take down, disable access to, restrict, suspend, or block specifically identified content, accounts, pages, groups, channels, features, applications, services, internet assets, URLs, domains, subdomains, or network access points demonstrably used to commit or facilitate violations of this Act, including where necessary through partial or feature-specific restrictions when technically feasible, and to the extent consistent with the principles of necessity, proportionality, technical feasibility, and the best interests of the child.

Where the order pertains to specifically identified CSAEM content, the concerned regulator may direct its removal, takedown, or disablement, and such content shall remain removed, taken down, or disabled unless otherwise ordered by the proper court or shown, upon review in accordance with applicable procedures, not to fall within the coverage of this Act.

Where the order pertains to the blocking, restriction, suspension, or other limitation of access to an account, page, group, channel, feature, application, service, internet asset, URL, domain, subdomain, or network access point, such order shall be temporary and preventive in character and shall remain effective for a period not exceeding thirty (30) days from service or implementation, unless earlier lifted or modified.

In cases of imminent risk of harm to a child, manifest CSAEM, or ongoing OSAEC/CSAEM activity requiring immediate intervention, the concerned regulator may issue an order under this paragraph *ex parte* or without prior notice and hearing, when necessary to prevent, disrupt, or stop the harm. In such a case, the covered entity shall be served the order and shall be given a prompt opportunity, within a period to be prescribed in the IRR, to submit a response, show compliance, seek modification or partial lifting, or contest the factual or technical basis of the order. The concerned regulator shall conduct prompt post-issuance review in accordance with the IRR and may modify, lift, or maintain the order, in whole or in part, based on the evidence and the principles of necessity, proportionality, technical feasibility, and the best interests of the child.

No administrative blocking, restriction, suspension, or other limitation of access issued under this paragraph shall remain in force beyond thirty (30) days unless, before the expiration of such period, the concerned regulator files the appropriate verified petition before any family court, seeking the continuation, extension, modification, or permanent imposition of such measure.

For purposes of this paragraph, the petition may be filed before any family court in the Philippines, without need to establish, at that stage, the precise place where the content was uploaded, where the relevant computer system, service, platform, or internet asset is physically situated, where the child victim resides, or where the harm occurred.

Where multiple petitions involving the same subject matter are filed, the court where the petition is first filed and raffled shall acquire jurisdiction to the exclusion of the others, without prejudice to consolidation where proper under applicable rules.

The designated family court shall act on the petition within five (5) days from raffle, on the basis of the verified petition, supporting evidence, and any comment or opposition that the court may require within a non-extendible period to be fixed by the court, consistent with the urgent nature of the proceedings.

Only the proper court may authorize the continuation of a blocking, restriction, suspension, or similar access-limitation measure beyond thirty (30) days, or its permanent imposition, upon a finding, after observance of due process and applicable rules, that such measure remains necessary, proportionate, technically feasible, and consistent with the best interests of the child.

An order of the family court affirming, extending, modifying, or permanently imposing a blocking, restriction, suspension, or similar access-limitation measure under this paragraph shall be immediately executory notwithstanding appeal, without prejudice to the power of the Court of Appeals or the Supreme Court to issue injunctive relief in accordance with law and the Rules of Court.

Unless extended, modified, or replaced by order of the proper court, an administrative blocking, restriction, suspension, or similar access-limitation order issued under this paragraph shall automatically lapse upon the expiration of the thirty (30)-day period.

Except as provided in the immediately preceding paragraphs, no final adverse order shall be issued under this paragraph without due notice and opportunity to be heard.

(d) Preservation Directives. – Issue a written directive requiring the preservation of specified data, logs, metadata, transaction records, account information, or other relevant digital evidence for a period and in a manner consistent with this Act, Republic Act No. 10175, Republic Act No. 10173, and other applicable laws. The authority granted under this paragraph is in addition to, and not in substitution for, any authority vested by law in any law enforcement agency, prosecutorial office, or other competent authority to issue or seek preservation orders, requests, or directives, or otherwise require the preservation of computer data or related records, including under Republic Act No. 10175, its IRR, and other applicable laws.

The authority granted under this paragraph is in addition to, and not in substitution for, any authority vested by law in any law enforcement agency, prosecutorial office, or other competent authority to issue or seek preservation orders, requests, or directives, or otherwise require the preservation of computer data or related records, including under Republic Act No. 10175, its IRR, and other applicable laws.

(e) Administrative Fines. – Impose an administrative fine in an amount, range, or scale to be specified in the IRR, taking into consideration the attendant circumstances, including:

(1) The nature and gravity of the violation;

(2) The duration and frequency of the violation;

(3) The number of children affected or placed at risk;

(4) The size, nature, and financial capacity of the person or entity concerned;

(5) The degree of cooperation during investigation or compliance review;

(6) Remedial measures taken;

(7) Previous administrative or criminal liability; and

(8) Other analogous circumstances.

The IRR may provide for graduated fine ranges depending on the type of covered entity, the nature of the duty violated, and whether the violation is first-time, repeated, willful, systemic, or involves unjustified refusal to comply with lawful orders.

(f) Censure or Formal Reprimand. – Issue a written censure or formal reprimand, which may be taken into account as an aggravating factor in subsequent violations.

(g) Suspension, Non-Renewal, or Revocation of Permits and Licenses. – Order, recommend, or refer to the issuing authority, as appropriate, the suspension, non-renewal, revocation, restriction, or other appropriate action on permits, licenses, authorizations, registrations, accreditations, franchises, certificates of authority, or other authority to operate, in cases of serious, repeated, or willful violations, or unjustified refusal to comply with lawful orders issued under this Act.

(h) Other Analogous Sanctions. – Such other analogous or incidental administrative sanctions as may be provided in the IRR or sectoral regulations, consistent with the objectives of this Act and with due process requirements.

SEC. 46. ***Determination of Appropriate Sanction.*** – In determining the appropriate sanction or combination of sanctions, the concerned regulator shall be guided by the principles of necessity and proportionality, taking into account the best interests of the child, the seriousness and systemic nature of the violation, the respondent's role in the OSAEC/CSAEM ecosystem, the respondent's compliance history, and the need to deter future violations.

SEC. 47. ***Due Process, Review, and Coordination.*** – All final orders and sanctions issued under this chapter shall be in writing, shall state the factual and legal basis therefor, and shall be subject to review in accordance with applicable law

and rules. The respective regulators shall prescribe procedures for notice, response, post-issuance review in exigent cases, documentation, audit trails, and lifting or modification of orders, including measures to ensure child-sensitive data protection, evidence preservation, and safeguards against overbreadth.

SEC. 48. ***Service Clause.*** – Service of administrative orders and judicial petitions under this chapter shall be made on the designated Philippine legal representative of the covered entity; in the absence, non-designation, unavailability, or refusal of such legal representative, service may be effected in accordance with the provisions of this Act on alternative service, and such absence, non- designation, unavailability, or refusal shall not prevent the issuance, enforcement, or judicial continuation of orders under this section.

SEC. 49. ***Without Prejudice to Existing Powers.*** – Nothing in this chapter shall be construed to limit, diminish, or otherwise prejudice the existing regulatory, supervisory, or sanctioning powers of the NTC, DICT, BSP, SEC, NPC, DepEd, CHED, TESDA, DTI, LGUs, and other regulators under their respective charters and special laws. The administrative sanctions and order under this Act may be imposed in addition to, and not in substitution for, any sanctions or remedies available under such other laws.

SEC. 50. ***Prescription of Administrative Actions.*** – Administrative actions arising from violations of this Act or its IRR shall prescribe within ten (10) years, counted from the date of discovery thereof or from the date the child reaches the age of majority, whichever occurs later.

The issuance of a show-cause order, notice of violation, compliance order, preservation directive, or any formal commencement of an administrative investigation shall interrupt the prescriptive period.

For continuing violations, the prescriptive period shall run only from the date the unlawful conduct or non-compliance ceases.

SEC. 51. ***Periodic Reporting.*** – All agencies exercising regulatory authority pursuant to this chapter shall submit periodic reports to the NCC, through the NC–COpS, on the status and disposition of administrative actions, compliance orders, investigations, enforcement measures, and related proceedings undertaken within their respective mandates.

The NCC shall prescribe the frequency, format, and required data fields of said reports.

CHAPTER VII
Financial and Regulatory Oversight

SEC. 52. ***Treatment as Unlawful Activity under the Anti-Money Laundering Act.*** – Violations of the penal provisions of this Act shall be considered unlawful activities under Section 3(i) of Republic Act No. 9160, otherwise known as the Anti-Money Laundering Act of 2001, as amended, and shall be subject to the provisions, remedies, powers, duties, and penalties under said Act.

Any reference in Republic Act No. 9160, as amended, its implementing rules and regulations, or related issuances to violations of Republic Act No. 11930 shall be deemed to refer to the corresponding offenses and violations under this Act.

SEC. 53. ***Temporary Restriction, Hold, Suspension, or Deferral of Funds or Payment Facilities.*** – PSPs, VASPs, and other covered financial entities shall have the authority to temporarily restrict, hold, suspend, delay, or defer the processing, transfer, withdrawal, cash-out, conversion, settlement, or release of funds, transactions, accounts, wallets, payment instruments, merchant accounts, virtual asset services, payment facilities, or other payment-related services under their control, where there are reasonable grounds to believe that the same is being used, has been used, or is intended to be used in connection with any act punishable under this Act.

Reasonable grounds may arise from:

(a) A lawful order, request, report, referral, alert, or notice from a competent authority;
(b) Information lawfully received from another covered entity;
(c) A complaint or report from a child, parent, guardian, caregiver, or other informant; or
(d) Specific and documented indicators, red flags, typologies, alerts, or findings generated through the covered entity's risk-based monitoring, screening, compliance, trust and safety, or internal detection systems.

The BSP shall issue rules and regulations on:

(a) The circumstances under which entities are required to exercise such authority to avoid facilitating OSAEC-CSAEM related transactions;
(b) The grounds for, procedure, and period of holding, deferring, suspending of funds; the period wherein the entities should notify the BSP whenever it holds funds;
(c) The verification and validation process; the release of funds subject of a flagged transaction; and

(d) Other actions that may be undertaken by the entities and parties to the flagged transaction during the period of temporary holding of funds.

SEC. 54. ***Freezing of Monetary Instruments or Property.*** – The temporary suspension and freezing of monetary instruments or property related to violations of this Act shall be governed by Republic Act No. 9160, otherwise known as the Anti-Money Laundering Act of 2001, as amended, and its IRR.

Temporary restriction, holding, suspension, delay, or deferral undertaken by a covered financial entity under the immediately preceding section of this Act shall be without prejudice to, and shall not be deemed a substitute for, any freeze order, civil forfeiture, asset preservation, or other remedy under Republic Act No. 9160, as amended, or other applicable laws.

SEC. 55. ***Authority to Inquire into Bank Deposits, Financial Accounts, and Transactions.*** – The authority of the AMLC to inquire into or examine bank deposits, investments, financial accounts, monetary instruments, property, and related transactions in connection with violations of this Act shall be governed by Republic Act No. 9160, otherwise known as the Anti-Money Laundering Act of 2001, as amended, its IRR, and other applicable laws.

SEC. 56. ***Coordination of AMLC and Competent Authorities.*** – Upon the commencement of any inquiry regarding bank deposits, financial transactions and financial accounts or the suspension of transactions and freezing of monetary instruments or properties due to suspicion of involvement in OSAEC or CSAEM-related activities, the AMLC shall ensure proper referral and coordination of the subject accounts to competent authorities for the conduct of appropriate investigation proceedings.

CHAPTER VIII
Victim Protection and Support

SEC. 57. ***Protective Custody of the Child.*** – Upon reasonable suspicion that a child is a victim or potential victim of any offense punishable under this Act, including attempted offenses, a law enforcement officer or a duly authorized social welfare officer may immediately place such child under temporary protective custody of the city or municipal social welfare and development office, or any accredited or licensed child-caring or child-placement agency, for the purpose of ensuring the child's safety, protection, and access to appropriate intervention services. Such placement shall be without prejudice to the conduct of appropriate assessment, rescue operations, and the initiation of formal custody proceedings in accordance with existing child protection laws.

Upon initial assessment or validation that the child is a victim of any offense under this Act, the child shall be immediately placed under the protective custody of the city or municipal SWDO: *Provided,* That in cases where (a) the city or municipal SWDO has no registered social worker that can perform case management; (b) the LGU does not have any residential care facility that can afford center-based intervention and rehabilitation; and/or (c) it was assessed that there are safety and risk factors detrimental to the child's stay in the same locality, the DSWD shall provide support and assistance to the concerned city or municipal SWDO by assuming temporary protective custody over the child: *Provided, however*, That the needs of the child shall be provided for by the concerned LGU: *Provided, further*, That the custody proceedings shall be in accordance with the provisions of Presidential Decree No. 603, otherwise known as "The Child and Youth Welfare Code."

Where probable cause exists in OSAEC/CSAEM cases, the DSWD or the Municipal/City Social Welfare and Development Office, in coordination with law enforcement authorities, shall immediately take custody of the victims. Any person who obstructs the implementation of such rescue operations shall be held liable for obstruction of justice.

The DSWD and the DOJ shall extend all necessary legal assistance and support to the city or municipal SWDO for any legal impediment that may arise in performing their functions in assuming temporary protective custody as another form of technical assistance and resource augmentation. In the regular performance of this function, the city or municipal SWDO or the DSWD shall be free from any administrative, civil or criminal liability.

The child shall also be considered as a victim of a violent crime defined under Section 3 (d) of Republic Act No. 7309, otherwise known as "An Act Creating a Board of Claims under the Department of Justice for Victims of Unjust Imprisonment or Detention and Victims of Violent Crimes and for Other Purposes," and may claim compensation therefor

SEC. 58. *Mandatory Immediate and Continuing Services to Victims of Child Sexual Abuse or Exploitation.* – To ensure the safety, recovery, rehabilitation, and reintegration of child victims of sexual abuse or exploitation, concerned government agencies and LGUs, through the city or municipal SWDO, shall make available immediate and continuing services to child victims and, when appropriate, their families.

Within forty-eight (48) hours from contact with the child, the concerned agency or LGU shall provide immediate protection and stabilization services, including:

(a) Emergency protection, safety planning, rescue coordination, and referral to appropriate services;

(b) Comprehensive assessment of the child's physical, psychological, social, developmental, disability-related, educational, legal, and protection needs;

(c) Emergency shelter or appropriate housing in accredited facilities that provide child-sensitive, trauma-informed, and disability-inclusive care;

(d) Medical assessment and care, including sexual and reproductive health assessment and services, psychiatric care, physical rehabilitation, and other urgent health interventions warranted by the condition of the child;

(e) Psychological first aid and initial psychosocial support to assist the child in managing disclosure, distress, and immediate protection needs; and

(f) Initial legal assistance, including information on the child's rights, available remedies, complaint procedures, compensation mechanisms, and protection measures in a language and manner understood by the child.

The following services shall be provided on a continuing basis, as may be necessary, until recovery, rehabilitation, reintegration, safe case transition, or case closure, taking into account the best interests, safety, evolving capacities, and expressed needs of the child:

(a) Sustained counseling, psychosocial support, psychiatric care, medical care, sexual and reproductive health services, physical rehabilitation, and other health-related interventions;

(b) Free legal services and child-sensitive legal support, including assistance in sworn statements, forensic interviews, case preparation, court accompaniment, testimony through available child-protection procedures, qualified interpreters or special educators when necessary, and continuing support throughout investigation, prosecution, and trial;

(c) Financial assistance for fees and expenses related to legal proceedings, immediate care, protection, recovery, rehabilitation, and reintegration, in accordance with applicable laws, guidelines, and referral mechanisms;

(d) Educational assistance, including school reintegration support, alternative learning systems, flexible learning arrangements, and scholarships;

(e) Livelihood, skills training, and economic support for the child, when of legal age, and for the child's family or caregivers, where appropriate, to reduce vulnerability to re-exploitation;

(f) Family assessment, family strengthening, parenting support, and community-based services, where safe and appropriate; and

(g) Other recovery, rehabilitation, reintegration, aftercare, and protection services necessary to prevent re-victimization, retaliation, stigma, abandonment, or re-exploitation.

A sustained supervision and follow-through mechanism shall be adopted through structured case management and post-reintegration monitoring, including periodic risk assessment and safety planning to prevent re-trafficking, re-victimization, retaliation, or further harm.

The DSWD and other concerned national government agencies shall provide technical assistance, standards, monitoring, and resource augmentation to LGUs and accredited institutions. Funding for the implementation of this section shall be included in the annual budgets of concerned agencies and LGUs.

SEC. 59. ***Programs for Victims of Child Sexual Abuse or Exploitation.*** – The NCC shall develop, coordinate, and monitor national programs for the prevention of child sexual abuse or exploitation, the protection of child victims and survivors, and their recovery, rehabilitation, reintegration, and long-term safety.

Such programs shall include:

(a) National and local prevention, awareness, and education programs on OSAEC, CSAEM, digital safety, reporting mechanisms, and help-seeking behavior;
(b) National research, data collection, monitoring, evaluation, and learning programs on OSAEC, CSAEM;
(c) Technical, material, capacity-building, and resource support to government agencies, local government units, accredited institutions, civil society organizations, and other partners;
(d) Conferences, consultations, trainings, writeshops, and other platforms for inter-agency coordination, consensus-building, and partnership with academe, civil society, development partners, international organizations, private sector, and other stakeholders;
(e) Mandatory integration of OSAEC-CSAEM cases in matters deliberated by the Regional Peace and Order Council (RPOC), City Peace Order and Council, and Municipal Peace and Order Council (MPOC) throughout the country;
(f) Survivor-centered, trauma-informed, disability-inclusive, culturally responsive, and rights-based frameworks, standards, and tools for prevention, investigation support, prosecution support, healing, reintegration, aftercare, and post-reintegration monitoring;

(g) Safe, ethical, meaningful, and trauma-informed mechanisms for survivor participation in advisory, consultation, policy, program design, monitoring, or evaluation processes;
(h) Long-term reintegration and resilience programs, including family strengthening, education continuity, livelihood and economic support, community-based services, digital safety support, and measures to reduce the risk of re-victimization, stigma, retaliation, or abandonment; and
(i) Continuing digital protection and recirculation response mechanisms to address the circulation, reupload, redistribution, resurfacing, or technological manipulation of abusive digital content involving the child victim or survivor, including accessible reporting channels and active assistance in coordinating lawful takedown, delisting, restriction, preservation, and cross-border referral processes.

The burden of monitoring, reporting, or pursuing the removal of abusive content shall not be shifted to the child victim or survivor. Digital protection, recirculation response, and digital reintegration mechanisms shall remain available beyond initial case disposition and shall form part of long-term aftercare and reintegration support.

The IRR shall prescribe the programs, standards, lead and support agencies, coordination mechanisms, referral arrangements, monitoring indicators, and funding support necessary to implement this section.

SEC. 60. ***Reasonable Accommodation for Children with Disabilities.*** – The DOJ and DSWD shall develop and update the guidelines, pursuant to the United Nations (UN) Convention on the Rights of Persons with Disabilities, for the provision, as far as practicable, of necessary and appropriate modification and adjustments across all stages of case management of OSAEC cases to ensure children with disabilities will have access to justice.

The Supreme Court shall, in accordance with its rules and the UN Convention on the Rights of Persons with Disabilities, issue guidelines for the provision, as far as practicable, of necessary and appropriate modification and adjustments across all stages of case management of OSAEC and CSAEM cases to ensure children with disabilities will have access to justice.

The National Council on Disability Affairs (NCDA) shall lead the implementation of the guidelines issued, developed and updated under this section.

SEC. 61. ***Care, Protection, and Psychological Well-Being of Multi-Disciplinary Team (MDT) Members and Other Government Personnel Serving as Frontliners in Reporting and Handling OSAEC and CSAEM Cases.*** – In recognition of the psychosocial risks involved in reporting, investigating, prosecuting, rescuing, and managing OSAEC and CSAEM cases, national government agencies,

LGUs, law enforcement agencies, prosecution offices, social welfare authorities, and other entities whose personnel serve as members of multidisciplinary teams or frontline responders shall establish, fund, and sustain a trauma-informed care and wellness program for such personnel.

The program shall include regular psychological debriefing, counseling, peer support, crisis intervention, wellness and stress-management activities, training on self-care and trauma recognition, and access to psychological first aid. Personnel who manifest vicarious trauma, secondary traumatic stress, compassion fatigue, or burnout, as assessed by a qualified mental health professional, may be granted temporary respite, reassignment, or workload adjustment without prejudice to their employment status, seniority, benefits, or pay.

Agencies shall adopt reasonable rotation, workload-management, and supervisory mechanisms to prevent prolonged or unmitigated exposure to traumatic materials, disclosures, investigations, or casework. The IRR shall prescribe minimum standards, frequency, responsible offices, confidentiality safeguards, and funding arrangements for the implementation of this section.

CHAPTER IX
Registries, Referral Systems and Data Management

SEC. 62. *Creation of the Philippine Child Sex Offenders Registry.* – A Philippine Child Sex Offenders Registry accessible to the public shall be created and lodged in the NC-COpS.

(a) Coverage and inter-related offenses. – The registry shall cover adult individuals convicted with finality of: (i) offenses under this Act, and (ii) other sexual offenses against children, whether committed in-person or online, and whether technology-facilitated or not, in recognition that offline child sexual abuse and online sexual abuse and exploitation are interrelated and may involve the same offender behaviors, grooming patterns, and victimization pathways.

For purposes of this section, "other sexual offenses against children" refers to offenses where the victim is a child and the act constitutes sexual abuse, sexual exploitation, or sexual violence, including but not limited to acts penalized under the Revised Penal Code and special laws on child sexual abuse and exploitation, even when the commission of the offense does not involve the use of ICT. The IRR shall provide the specific list of covered offenses and the operational cross-references.

(b) Minimum information accessible to the public. – The registry shall contain, at a minimum, information necessary for identification, risk management, and child safeguarding, including:

(1) Name, including aliases;
(2) Photograph;
(3) General location of the offender; and
(4) Tier classification of crime, as determined in the tiered classification framework to be adopted through this Act.

(c) Tier classification and monitoring. – The NCC shall adopt a tiered classification framework for registry subjects, based on seriousness of offense and other risk factors, to guide monitoring intensity, verification frequency, and eligibility for delisting, as provided in the IRR.

(d) Mandatory Information-Sharing for Registry Purposes. – The NC-COpS, the Supreme Court and lower courts, the Bureau of Corrections, the Bureau of Jail Management and Penology, law enforcement agencies, prosecution offices, parole and probation authorities, local civil registrars, and other relevant government agencies shall share, transmit, validate, and update information necessary for the establishment, maintenance, verification, and updating of the Philippine Child Sex Offenders Registry.

Such information shall include conviction, detention, confinement, release, transfer, supervision, registration, identity, address, case status, and other relevant registry information, in the form, manner, frequency, and safeguards prescribed in the implementing rules and regulations.

(e) Updating and verification. – The registry shall be regularly updated. The IRR shall prescribe initial registration, periodic in-person verification, and change-of-information reporting requirements.

(f) Delisting and reinstatement. – The IRR shall prescribe criteria and procedures for delisting, including risk assessment, due process safeguards, and reinstatement upon violation of delisting conditions or commission of specified offenses. Delisted records may be retained as inactive records subject to strict access controls, for child safeguarding purposes.

(g) Administrative liability for failure to implement registry safeguarding obligations. – Any child-serving institution, employer, licensing body, accrediting entity, or regulator required to conduct registry clearance or enforce registry-based disqualification which, through gross negligence or willful disregard, fails to comply with such obligation shall be subject to administrative sanctions.

Sanctions shall include fines, suspension or revocation of license or accreditation, and other penalties as may be prescribed in the IRR.

SEC. 63. ***Blacklisting of Alien OSAEC Offenders.*** – The Bureau of Immigration (BI) and the DOJ, in coordination with the Department of Foreign Affairs (DFA), shall ensure that all convicted offenders of OSAEC, CSAEM, and other sexual offenses against children or similar or equivalent crimes in other jurisdictions, or those aliens reported to or being monitored by Philippine and foreign law enforcement authorities for conducting OSAEC, CSAEM or other sexual offenses, or those aliens who pose a serious risk of committing OSAEC, CSAEM offenses, or other sexual offenses involving children, shall not be allowed entry in the Philippines.

In addition to its data system collection and database functions under section, the NC-COpS shall create and maintain an updated registry of blacklisted aliens based on the information from the DFA, BI, DOJ-National Prosecution Service, DOJ-Legal, local and foreign law enforcement authorities, foreign or international child-protection partners, international clearinghouses and cybertiplines, foreign sex offender registries or equivalent databases, International Criminal Police Organization (INTERPOL) notices, and such other reliable information, including open- source materials such as official public registries, court decisions, government websites, and reports from reputable news or media organizations, as may be further defined in the IRR.

For this purpose, and without prejudice to other grounds for exclusion or deportation under existing laws, the BI, in coordination with the DOJ and DFA, may deny entry, cancel or refuse visa issuance or renewal, or order the exclusion or deportation of aliens included in the blacklist.

SEC. 64. ***Referral Pathway for OSAEC Cases.*** – There shall be an organized and unified referral pathway and a national public-facing reporting entry mechanism for or OSAEC, CSAEM, and related technology-facilitated child sexual abuse or exploitation cases.

The NCC shall establish policy direction, standards, and protocols for the unified referral pathway, including uniform intake, triage, documentation, referral timelines, confidentiality safeguards, reporter and victim-survivor feedback, data recording, case monitoring, and child-sensitive, trauma-informed, and victim-centered coordination among law enforcement agencies, prosecutors, social welfare authorities, health facilities, schools, local government units, and other competent authorities.

There shall be one national helpline that shall serve as the primary public-facing reporting entry mechanism, operating twenty-four (24) hours a day, seven (7) days a week, and providing accessible reporting channels through

telephone, digital, and other accessible channels. This shall be without prejudice to other agencies and mechanisms authorized to receive complaints or reports under existing laws. Reports received through the helpline shall be promptly referred, triaged, and coordinated under the unified referral pathway.

The DOH, in coordination with the NCC, shall ensure that at least one operational Women and Children Protection Unit is established or designated in every province and highly urbanized city, subject to phased implementation as may be provided in the IRR.

The DepEd, in coordination with the NCC, DICT, DSWD, DOH, and other relevant agencies, shall integrate age-appropriate and child-sensitive digital safety, online child protection, and OSAEC and CSAEM prevention education into the basic education curriculum, including prevention and help-seeking behavior. It shall likewise establish capacity-building programs to teachers and school personnel in the identification, detection, and reporting of OSAEC-CSAEM cases or incidents.

The DILG shall support capacity-building of LGUs and barangay officials to act as first responders and facilitate local implementation of the unified referral pathway.

The NC-COpS, in coordination with the DOJ, DILG, PNP, NBI, DSWD, DOH, DepEd, LGUs, and other relevant agencies, shall issue and periodically update implementing guidelines for referral coordination, inter-agency case management, digital evidence preservation, first-responder protocols, local implementation, school-based reporting, health and protection referrals, aftercare coordination, and prevention and awareness initiatives.

CHAPTER X
Cooperation and Information Sharing

SEC. 65. ***Handling of Cybertipline Reports and International Child-Protection Hotlines.*** –

(a) Scope. – This section shall apply to reports, referrals, or notifications relating to OSAEC and/or CSAEM transmitted by foreign or international child-protection hotlines, clearinghouses, specialized databases, or similar entities that function as centralized reporting or triage hubs for child sexual abuse or exploitation material, including but not limited to the National Center for Missing and Exploited Children (NCMEC) cybertipline or their successors.

(b) National Clearinghouse; Point-of-Contact. – The NC-COpS shall serve as the National Point-of-Contact and clearinghouse for OSAEC and CSAEM reports covered by this section for purposes of receipt, logging, triaging, risk assessment,

de-duplication, national-level deconfliction, referral, monitoring, and analytics, subject to applicable confidentiality, data-privacy, and information-security rules.

For this purpose, the NC-COpS may enter into arrangements, protocols, or data-sharing and coordination mechanisms with other competent authorities to assist in the receipt, access, triage, prioritization, deconfliction, referral, assignment, monitoring, and disposition of such reports and referrals, subject to approved referral protocols, data protection safeguards, confidentiality requirements, and applicable laws.

(c) Transitory Provision on Existing Foreign Referral and Database Mechanisms. – Upon the effectivity of this Act, the NC-COpS and the concerned government agencies or competent authorities currently managing or accessing foreign referral, CyberTipline, hotline, clearinghouse, international database, secure network, or analogous mechanisms involving OSAEC, CSAEM, or related technology-facilitated child sexual abuse or exploitation with a Philippine nexus shall establish shared management, shared access, or interoperable access arrangements over the relevant accounts, portals, access privileges, records, reports, and pending referrals.

Such arrangements shall remain in force until the full referral, transfer, integration, or migration of the foregoing to the NC-COpS, to the extent permitted by applicable governing rules, access conditions, agreements, protocols, or arrangements, and subject to data protection, confidentiality, cybersecurity, and child protection safeguards.

SEC. 66. ***Cooperation with Foreign Law Enforcement; Retention and Sharing of Evidence in OSAEC and CSAEM Cases.*** – Recognizing the transnational and technology-facilitated nature of OSAEC and CSAEM, Philippine law enforcement agencies shall, as part of their investigative protocols, assess whether a case has a foreign nexus, including through available digital, technical, platform-related, financial, communications, referral, travel, or other relevant indicators.

Where the facts indicate or reasonably suggest a foreign nexus, Philippine law enforcement agencies may, consistent with this Act and other applicable laws, directly exchange operational information, referrals, intelligence, digital forensic results, and other relevant case information with competent foreign law enforcement authorities, designated 24/7 points of contact, international police cooperation channels, foreign hotlines, clearinghouses, child-protection reporting mechanisms, and analogous entities, for purposes of identifying and safeguarding victims, identifying offenders, preserving evidence, conducting case build-up, and undertaking parallel or joint investigations.

Notwithstanding Sections 15 and 16 of Republic Act No. 10175, law enforcement authorities may securely retain copies of computer data acquired or seized, results of digital forensic examination or analysis, and other evidence lawfully obtained in OSAEC or CSAEM cases, including materials obtained pursuant to a warrant, subpoena, voluntary consent, or other lawful process, for purposes of victim identification and safeguarding, offender identification, further investigation, case build-up, prosecution, and lawful domestic or cross-border cooperation.

Law enforcement authorities may share such retained evidence, including certified copies and accompanying certifications, with competent foreign law enforcement authorities, designated 24/7 points of contact, international police cooperation channels, or other competent foreign authorities for use in investigations or judicial proceedings abroad: Provided, That the evidence was lawfully obtained; use-limitations, data-minimization, confidentiality, and child-protection safeguards are observed; and personally identifiable information of child victims and other sensitive victim data are protected, including through redaction or other protective measures where appropriate.

Direct or expedited law enforcement cooperation under this section shall not preclude recourse to mutual legal assistance, extradition, formal service of process, compelled production of evidence abroad, testimony-taking, asset restraint, or other State-to-State processes where required by applicable law, treaty, or the domestic law of the receiving jurisdiction. Materials shared through direct channels may be regularized through mutual legal assistance where necessary or upon request.

Evidence retained under this section shall be kept only for as long as reasonably necessary for the purposes stated herein, or as otherwise required by law, court order, or preservation obligation, after which secure deletion or lawful disposition shall be undertaken.

The IRR shall prescribe procedures, safeguards, templates, certifications, use-limitations, retention periods, disposition procedures, protective measures, and coordination protocols necessary to implement this section.

SEC. 67. ***Inter-Agency Information-Sharing and Shared Data Systems in OSAEC and CSAEM Cases.*** – Domestic law enforcement agencies, prosecution offices, and other investigative bodies mandated to investigate, assist in the investigation of, or prosecute OSAEC and CSAEM cases shall, subject to their respective mandates and applicable legal restrictions, shall share with one another timely and relevant information necessary for victim identification, offender identification, rescue, referral, deconfliction, investigation, case build-up, prosecution support, and case monitoring.

Such agencies and offices shall, to the extent consistent with law and their respective functions, participate in and contribute to authorized shared databases, case-tracking systems, and the Data Fusion Center established or coordinated by the NC-COpS, including by submitting, updating, validating, accessing, and using relevant reports, referrals, case information, analytical products, and status updates necessary for the effective implementation of this Act.

Information-sharing may be undertaken on the agency's own initiative or upon request, and may be effected through direct coordination, through the NC-COpS and its authorized systems, or, for cases with a foreign nexus, through PICACC in accordance with its mandate and approved protocols.

Nothing in this section shall be construed to require the disclosure of information where such disclosure would compromise an ongoing operation, endanger a child victim or witness, violate a lawful restriction, or bypass specialized information-sharing, financial intelligence, or other frameworks under applicable law.

The IRR, inter-agency protocols, or data-sharing agreements shall prescribe the minimum data elements, timelines, focal points, access levels, safeguards, and accountability mechanisms for information-sharing and participation in shared systems under this section.

The duty to cooperate and designate focal persons shall be immediately effective upon the effectivity of this Act. Actual data-sharing through shared systems shall be undertaken in accordance with minimum safeguards on purpose limitation, role-based access, source-agency control, confidentiality, audit trails, retention, and child protection, as may be prescribed in the IRR, interim protocols, or data-sharing agreements.

SEC. 68. ***National Financial Intelligence Fusion Platform Against OSAEC and CSAEM.*** – A secure National Collaborative Intelligence Platform headed by and lodged in the BSP is hereby established to enable the near real-time sharing and joint analysis of financial intelligence for the detection of OSAEC and CSAEM-related financial activity, the generation of investigative leads, and the enhancement of analytical products that directly support timely law enforcement, regulatory, protective, and disruption action under this Act. This shall include the responsible development and use of algorithms to detect patterns of digital and financial behavior associated with OSAEC, which financial institutions and PSPs may deploy to flag suspicious transactions or activities, promptly refer actionable intelligence to competent authorities, and, where authorized under this Act or other applicable laws, take timely preventive or disruption measures, including the temporary restriction, hold, suspension, delay, or deferral of funds or payment facilities.

The Platform shall connect relevant law enforcement, regulatory, and government agencies, financial institutions, and payment service providers for the purpose of identifying, tracing, disrupting, and investigating individuals, accounts, networks, and financial channels reasonably suspected of involvement in OSAEC and CSAEM, and to ensure that shared intelligence and algorithm-generated alerts are translated into timely investigative and enforcement action, including prompt action by participating covered entities and competent authorities, as may be authorized under this Act or other applicable laws.

Relevant agencies and covered entities shall be required to participate in and maintain connectivity to the Platform in accordance with standards and protocols to be prescribed in BSP circulars. The Platform shall likewise serve as a data fusion center where participating agencies and entities can continuously develop, test, validate, and refine analytical products, including algorithmic detection tools, to strengthen investigative capacity, support evidence-building, and improve case outcomes for agile law enforcement and effective prosecution, as well as to support the timely identification of suspicious financial activity requiring referral or action under this Act.

Participation in the Platform and the good faith sharing of financial intelligence pursuant to this section shall not give rise to civil, criminal, or administrative liability, provided that such sharing is lawful, necessary, proportionate, and consistent with applicable confidentiality, banking secrecy, and privacy laws.

The IRR to be issued by the BSP within six (6) months from passage of this Act, and succeeding BSP circulars as necessary, shall prescribe the technical, operational, and security safeguards required to ensure the confidentiality, integrity, availability, and lawful use of financial intelligence shared through the Platform.

SEC. 69. ***Extradition and Mutual Legal Assistance.*** – The DOJ shall be the central authority for all requests for extradition and mutual legal assistance in all legal matters: *Provided,* That the government may surrender or extradite any person accused or convicted of child sexual abuse or exploitation pursuant to the extradition law and applicable extradition treaty.

The DOJ shall make and receive requests for mutual legal assistance in criminal matters from a foreign State relative to the investigation or prosecution of, related criminal proceedings to, any form of child sexual abuse or exploitation and execute or arrange for the execution of such request for assistance. In case there is an existing mutual legal assistance treaty between the Philippines and a foreign State, the provisions of that treaty shall apply.

CHAPTER XI
Final Provisions

SEC. 70. Congressional Oversight Committee. – There is hereby created a Congressional Oversight Committee composed of five (5) members from the Senate of the Philippines and five (5) members from the House of Representatives. The members of the Senate shall be composed of the Chairperson of the Senate Committee on Women, Children, Family Relations and Gender Equality and the remaining four (4) members shall be appointed by the Senate President. The members of the House of Representatives shall be composed of the Chairperson of the Committee on Public Order and Safety and the remaining four (4) members shall be appointed by the Speaker of the House of Representatives.

The Oversight Committee shall monitor and ensure the effective implementation of this Act, recommend the necessary remedial legislation or administrative measures, and perform such other duties and functions.

SEC. 71. *Transitory Provisions.* –

(a) Transfer of Functions, Assets and Personnel - All mandates, powers, functions, personnel, funds, assets, funds, equipment, properties, transactions, information and database of the National Coordination Center Against OSAEC and CSAEM (NCC-OSAEC-CSAEM), as the case may be, shall be transferred to the National Council for Child Online Safety and Protection, subject to the existing budgeting, accounting, auditing and other pertinent laws.

All the mandates, powers, functions, personnel, funds, assets, information and database of the NCC-OSAEC-CSAEM Secretariat, as the case may be, shall be transferred to the NC-COpS.

(b) Transition Period - The foregoing transfer and the formulation of the revised budget, and the internal organic structure, staffing pattern, and operating system of the NCC and the NC-COpS shall be completed within two (2) years from the effectivity of this Act.

The DOJ and the Executive Director of the NCC-OSAEC-CSAEM, in coordination with the DBM, shall determine the staffing pattern and funding requirements of the NCC and NC-CopS subject to the review and evaluation of the Department of Budget and Management in accordance with the civil service and other pertinent laws, rules and regulations.

(c) Retention and Placement of Personnel - All existing personnel of the NCC-OSAEC-CSAEM Secretariat shall be automatically transferred to the NC-COpS: *Provided,* That they shall continue to perform their duties and receive their salaries, benefits, and emoluments until the approval of the new staffing pattern and the issuance of appointments in accordance with civil service laws, rules, and regulations.

The absorption of personnel shall be undertaken without diminution of rank, salary, seniority, or other benefits, and all affected personnel shall enjoy security of tenure in accordance with existing laws.

Personnel not absorbed in the approved staffing pattern shall be entitled to separation or retirement benefits under applicable laws, rules, and regulations.

(d) Transfer of Funds - All appropriations, funds, and revenues of the NCC-OSAEC-CSAEM and its Secretariat shall be deemed automatically transferred to the NCC and NC-COpS and shall be used for the continued discharge of its functions, subject to existing budgeting, accounting, and auditing laws, rules, and regulations.

(e) Additional Personnel of Member Agencies and Local Government Units (LGUs) - Concerned member agencies and LGUs may propose organizational structure, staffing pattern, or additional plantilla positions, as may be necessary, subject to the evaluation and approval of the Department of Budget and Management or the Governance Commission for GOCCs, whichever is applicable, to ensure compliance with civil service and other pertinent laws, rules, and regulations.

(f) Acts or Omissions Under Prior Laws - Acts or omissions punishable under Republic Act No. 9775 or the *"Anti-Child Pornography Act of 2009"* committed prior to the effectivity of Republic Act No. 11930 shall continue to be governed by Republic Act No. 9775, notwithstanding its repeal, for purposes of investigation, charging, prosecution, trial, and adjudication. Acts or omissions punishable under Republic Act No. 11930 committed on or after its effectivity and prior to the effectivity of this Act shall continue to be governed by Republic Act No. 11930 for the same purposes.

(g) Pending Cases - All such cases and proceedings, whether pending upon the effectivity of this Act or filed thereafter, shall be resolved under the law applicable at the time of the commission of the offense. All offenses committed on or after the effectivity of this Act shall be governed by this Act.

SEC. 72. *Appropriations.* – The amount necessary for the initial implementation of this Act shall be charged against the current year's appropriations of the departments, agencies and GOCCs concerned. Thereafter, the funding of which shall be included in the annual General Appropriations Act and corporate operating budgets of the GOCCs concerned.

The LGUs concerned may provide the necessary funds for the purpose, in their respective annual budgets.

SEC. 73. *Suppletory Application of the Revised Penal Code.* – The Revised Penal Code shall be suppletorily applicable to this Act.

SEC. 74. *Implementing Rules and Regulations.* – Within ninety (90) days from the effectivity of this Act, the DOJ shall, in coordination with NC-COpS, DSWD, DICT, DILG, NTC, BSP, and CICC, and in consultation with relevant government agencies and stakeholders from the private sector, promulgate the necessary rules and regulations for the effective implementation of this Act.

The Implementing Rules and Regulations (IRR) shall be approved by the NCC within thirty (30) days from submission. The IRR shall take effect upon its publication in two (2) national newspapers of general circulation.

SEC. 75. *Separability Clause.* – If any part of this Act is declared unconstitutional or invalid, the other provisions not affected thereby shall continue to be in full force and effect.

SEC. 76. *Repealing Clause.* – Republic Act No. 11930 otherwise known as the *Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act* is hereby repealed. All laws, decrees, executive orders, administrative orders, rules and regulations, and other issuances or parts thereof inconsistent herewith are hereby repealed, amended or modified accordingly.

Upon the effectivity of this Act, all references to Republic Act No. 11930 in any law, rule, regulation, circular, issuance, order, contract, instrument, or other legal document shall be deemed references to this Act, insofar as the subject matter is continued, modified, expanded, or replaced herein.

SEC. 77. *Effectivity.* – This Act shall take effect fifteen (15) days after its publication in the *Official Gazette* or in a newspaper of general circulation.

Approved,