CONGRESS OF THE PHILIPPINES
NINETEENTH CONGRESS
Third Regular Session

S E N A T E

S. No. 2781

(In substitution of Senate Bill Nos. 67, 194, 298, 318, 334, 455, 625, 685, 974, 982, 1051, 1126, 1172, 1542, 1574, 1867, 1978, taking into consideration House Bill No. 7327)

PREPARED AND SUBMITTED JOINTLY BY THE COMMITTEES ON SCIENCE AND TECHNOLOGY; CIVIL SERVICE, GOVERNMENT REORGANIZATION AND PROFESSIONAL REGULATION; LOCAL GOVERNMENT; PUBLIC INFORMATION AND MASS MEDIA; AND FINANCE WITH SENATORS CAYETANO (A.P.), GO, ZUBIRI, POE, ESTRADA, ANGARA, GATCHALIAN, LAPID, REVILLA JR., VILLAR (M.), EJERCITO, VILLANUEVA, LEGARDA, VILLAR (C.), DELA ROSA, TOLENTINO, AND TULFO AS AUTHORS THEREOF

AN ACT INSTITUTIONALIZING THE TRANSITION OF THE GOVERNMENT TO E-GOVERNANCE, ESTABLISHING FOR THE PURPOSE THE E-GOVERNANCE ACADEMY, 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 "E-Governance Act".

SEC. 2. *Declaration of Policy.* – The State recognizes the vital role of information and communication in nation-building and the necessity of leveraging the power of information and communications technology (ICT) to drive national development and progress.

The State hereby adopts a policy to establish, foster, and sustain a digitally empowered and integrated government through the implementation of a regulated, secure, and robust information and communication system aimed at facilitating responsive and transparent online citizen-centered services, thereby optimizing the potential of open data for promoting economic growth while balancing the rights to freedom of information and data privacy of every Filipino.

SEC. 3. *Purposes and Objectives.* – The purposes and objectives of this Act are:

(a) Define the roles and responsibilities of various government agencies in the entire digital transformation

process and provide effective leadership in developing and promoting electronic government services and processes;

(b) Promote interoperability of government systems and processes through a consolidated process architecture, while allowing government agencies, offices, and instrumentalities to implement the proper controls and safeguards deemed appropriate on ICT and information assets;

(c) Provide citizen-centered government information and services, and improve public trust and citizen participation in the government;

(d) Enable access to government information and services, in accordance with the Constitution and relevant laws, while leveraging ICT and emerging technologies to enhance process efficiency, data security, and overall effectiveness;

(e) Strengthen transparency and accountability efforts of the national and local governments;

(f) Foster an informed and data-driven decision-making process for policymakers by utilizing data analytics results, among other pertinent factors;

(g) Strengthen resilience against information technology disruptions, including but not limited to cybersecurity attacks, by incorporating best practices both from public and private sectors, locally and internationally;

(h) Promote electronic transaction, particularly where mobility of citizens is restricted during disasters or pandemics;

(i) Foster job creation, promote sustainability, and ensure up-to-date qualification and competency standards of ICT positions within the government;

(j) Encourage sustainability and fortify manpower capabilities by continuously upskilling ICT professionals through the E-Governance Academy; and

(k) Reduce costs and burdens for businesses and other government entities.

SEC. 4. *Coverage.* – This Act shall apply to all executive, legislative, judicial and constitutional offices, including local government units (LGUs), state universities and colleges (SUCs), government-owned or -controlled corporations (GOCCs) and other instrumentalities, whether located in the Philippines or abroad, that provide services covering business- and non-business-related transactions as defined in this Act, subject to limitations under existing laws. This Act shall also cover back-end government operations within, between, and across agencies, government-to-government transactions, particularly those involving sharing and processing of data and information between and among government agencies for policy, planning, and decision-making purposes, and other government operations. Nothing in this Act shall be construed to derogate the fiscal and administrative autonomy and independence of government entities.

SEC. 5. *Definition of Terms.* – As used in this Act:

(a) *Application Programming Interfaces (APIs)* refers to an intermediary that allows interaction between applications, programs, software components, systems, hardware, and micro-services of different individuals or organizations;

(b) *Blockchain* is a shared, immutable ledger that facilitates the process of recording transactions and tracking tangible or intangible assets in a business network, where virtually anything of value can be tracked and traded, reducing risk and cutting costs for all involved;

(c) *Chief Information Officer (CIO)* refers to a senior officer responsible for the development, planning, and implementation of the government entity's information systems strategic plan (ISSP) or ICT plan, and management of the agency's ICT systems, platforms, and applications;

(d) *Critical Information Infrastructure (CII)* refers to the computer systems and/or networks, whether physical

or virtual, and/or the computer programs, computer data and/or traffic data that are vital to this country that the incapacity, destruction, or interference with such system and assets would have a debilitating impact on security, national or economic security, national health and safety, or any combination of those matters. Sectors initially classified as CIIs are the following: government transportation (land, sea, air), energy, water, health, emergency services, public finance, banking and finance, business process outsourcing, telecommunications, space, and media;

(e) *Digitization* refers to the process of encoding information or procedure into digital form that can be read and manipulated by computers;

(f) *Digitalization* refers to the process of using digital technologies to enhance the operations of the government, and provide new revenue and value-producing opportunities;

(g) *Digital Transformation* refers to the process of optimizing, reconstructing, and integrating digital technology into all areas of government, to maximize resource configuration, improve operational efficiency and innovation capability, and enhance value delivery to stakeholders;

(h) *E-Governance* refers to the use of ICT by the government to provide public services in a more friendly, convenient, affordable, efficient, and transparent manner. Further, it is the application of ICT for delivering government services through integration of various stand-alone systems, platforms, and applications between Government-to-Citizens (G2C), Government-to-Business (G2B), and Government-to-Government (G2G) services. It is often linked to back-office processes and interactions within the entire government framework;

(i) *E-Government* refers to the use of ICT by the government to enhance access to and delivery of

government services for an efficient, responsive, ethical, accountable, and transparent government;

(j) *ICT Assets* refer to any data, device, equipment, infrastructure, system, or component thereof, utilized to ensure or support the proper and efficient operation and implementation of ICT-related programs and delivery of ICT services;

(k) *ICT Plan* refers to the sum or set of goals, measures, strategies, agenda, budget, and timeline for the implementation of ICT programs and projects and the use of ICT , including digital platforms, to deliver public services or otherwise perform governmental functions;

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

(m) *Information Security Standards (ISS)* refers to generally acceptable security standards which aim to protect and secure the confidentiality, integrity,

availability, authenticity, and non-repudiation of information;

(n) *Information Systems Strategic Plan (ISSP)* refers to the three (3)-year plan that serves as the government entity's roadmap for using ICT as a strategic resource to support the attainment of its goals, mission, and vision. It is also a written expression that aims to coordinate national ICT plans, efforts, knowledge, information, resource-sharing, and database-building, and to link a government entity's ISSPs with national ICT goals;

(o) *Interoperability* refers to the ability of different operating and software systems, applications, and services to communicate and exchange data in an accurate, effective, and consistent manner to different platforms and agencies;

(p) *Nonbusiness-related transaction* refers to all other government transactions not falling under Section 4(c) of Republic Act No. 11032, or the "Ease of Doing Business and Efficient Government Service Delivery Act of 2018";

(q) *Privacy Engineering* refers to the integration of privacy concerns into engineering practices for systems and software engineering life cycle processes;

(r) *Privacy-by-Design* refers to an approach in the development and implementation of projects, programs, and processes that integrates safeguards that are necessary to protect and promote privacy into the design or structure; and

(s) *Privacy-by-Default* refers to a practice of applying the strictest privacy settings by default, without any manual input from the user, when a product or service has been deployed for public use.

CHAPTER II
IMPLEMENTING AGENCY

SEC. 6. *Role of the Department of Information and Communications Technology (DICT).* – The DICT shall be the lead implementing body and administrator of this Act. In accordance with applicable laws and rules, and subject to limitations provided by the Constitution, the DICT shall

ensure that all ICT projects in the Philippines shall be done in accordance with the National ICT Development Agenda and E-Government Master Plan, as provided under Republic Act No. 10844 or the "Department of Information and Communications Technology Act of 2015". For this purpose, the DICT shall establish measures to implement policies under this Act and ensure that all ICT projects in the Philippines, whether national or local, are harmonized with the overall ICT plans and in compliance with applicable standards. Accordingly, the DICT shall:

(a) Adopt a national policy and process that promotes innovations, supports start-ups, and facilitates the entry and adoption of technologies consistent with the goals of this Act;

(b) Support, advise, monitor, and guide government agencies in ensuring the quality, security, and reliability of their respective ICT infrastructure and services, in accordance with international or industrial standards, specifications, and best practices, and ensure the

interconnection or interoperability of ICT infrastructure, systems, and facilities when necessary to achieve the goals of this Act;

(c) Coordinate and/or collaborate with the private sector and enter into partnerships and joint ventures in accordance with the goals of this Act;

(d) Mandate and guide the adoption of policies and processes to ensure the implementation of this Act, including the adoption of a roadmap to provide a strategic and phased whole-of-government transformation to E-Government, with clear and identified milestones, and which explicitly defines the roles and responsibilities of covered government agencies, offices, and instrumentalities;

(e) Empower and guide the operations of ICT infrastructure, systems, and facilities, and in the exercise of such functions, in accordance with applicable laws and rules;

(f) In coordination with the Civil Service Commission (CSC), mandate government agencies, offices, and instrumentalities to comply with the minimum qualification and competency standards of ICT positions in the government and require government agencies, offices, and instrumentalities, to regularly report the status of compliance thereto;

(g) Engage technical and standards organizations and consult industry experts on matters requiring engineering inputs, enterprise architecture, and other highly specialized concerns;

(h) Where applicable, recognize the administrative autonomy provided by the Constitution to independent government agencies, offices, and instrumentalities in the implementation and enforcement of the foregoing;

(i) Develop, in accordance with applicable civil service laws and rules, consistent with the compensation and position classification system of the government, the competency and qualification standards of all ICT positions

in the government, and submit to the Department of Budget and Management (DBM) the: (1) proposal for the creation and updating of current civil service positions for ICT workers, which include cybersecurity, data governance, data privacy, and other ICT-related government positions; (2) the appropriate job levels and corresponding compensation rates aligned with the personnel needs of digitally transformed government and comparable with the prevailing industry rates; and (3) the qualifications standards, duties, and functions essential to the effective operation of government ICT infrastructure and systems: *Provided,* That government agencies, offices, and instrumentalities granted by law and by their charter with fiscal and administrative autonomy in the performance of their Constitutional and statutory mandates shall independently undertake, supervise, and regulate their own ICT projects and shall only be required to coordinate and report to the DICT for alignment of policy objectives;

(j) Ensure that E-Government programs and platforms are inclusive and accessible to persons with disabilities, as far as practicable; and

(k) Issue Performance Score Card on the compliance of the different agencies, LGUs, SUCs, GOCCs as provided under Section 4 hereof. Such Performance Score Cards shall only be advisory in nature.

SEC. 7. *The E-Governance Unified Project Management Office (EGov UPMO).* – Within one (1) year from the effectivity of this Act, the DICT shall establish a government-wide EGov UPMO, which shall cater to and address the portfolio, program, and project management needs of government agencies, to ensure that ICT projects across the government are managed with efficiency and agility, following international best practices and standards.

The DICT shall provide guidelines on the operation of the EGov UPMO and the qualifications of personnel under the EGov UPMO, who shall, at the minimum, obtain

internationally recognized certifications and a required number of units on Project Management, Program Management, IT Service Management, Enterprise Architecture, Information Security, Data Privacy, Risk Management, and other similar fields or specializations. For this purpose, the E-Governance Academy created under this Act shall ensure that courses, multimodal training, and certifications to develop this human resource are regularly offered.

The EGov UPMO shall be headed by the Undersecretary for E-Government of the DICT.

CHAPTER III
THE E-GOVERNMENT MASTER PLAN, PROGRAMS AND SYSTEMS

SEC. 8. *E-Government Master Plan.* – The DICT shall formulate and promote an E-Government Master Plan (EGMP) or its equivalent that will serve as a blueprint for the development and enhancement of all electronic government service processes and workforce to achieve

digital transformation in the bureaucracy, taking into consideration the Philippine Development Plan. An integrated framework shall be developed to provide the government enterprise architecture and operationalize the blueprint through programs and projects relating to E-Government, to fully realize the vision, goals, and objectives of the EGMP. The EGMP and the accompanying integrated framework shall be reviewed and updated every three (3) years or earlier as the need arises, in anticipation of disruptions, emergencies, crises, and new and emerging technologies.

To effectively implement E-Governance across the government, a whole-of-government approach shall be adopted for the formulation and promotion of the EGMP. This approach shall facilitate engagement primarily with government agencies, instrumentalities, GOCCs, LGUs, Regional Development Councils, ICT Councils, technical and standards organizations, and other relevant stakeholders to ensure the full and effective implementation of the country's E-Governance Agenda. All

E-Government Programs identified herein and in the future, as well as in the ISSP of each government entity, shall be subject to mandatory monitoring by the DICT for alignment with the EGMP and its integrated framework.

SEC. 9. *E-Government Programs (EGP).* – The DICT, in coordination with relevant government agencies, shall develop the following programs and systems that will be regularly updated in consultation with stakeholders and ensure that such programs and systems are compliant with standards imposed by relevant laws, rules, and regulations relating to data privacy and security, including but not limited to Republic Act No. 10173, or the "Data Privacy Act of 2012":

(a) Citizen Frontline Delivery Services Platform (CFDSP). – Services that are needed to facilitate business and non-business transactions on permitting, licensing, and the issuance of any privilege, right, reward, clearance, authorization, or concession, including business or non-business related frontline services enrolled in the existing

citizen's charter, corresponding back-end support services, and regulatory functions related to permitting, licensing, and the issuance of any privilege, right, reward, clearance, authorization, or concession shall be made efficient by integrating all agencies involved, such as the Philippine Statistics Authority (PSA), Department of Foreign Affairs (DFA), Land Transportation Office (LTO), Land Transportation Franchising and Regulatory Board (LTFRB), National Bureau of Investigation (NBI), Professional Regulation Commission, Department of Trade and Industry (DTI), Securities and Exchange Commission (SEC), *Bangko Sentral ng Pilipinas* (BSP), Cooperative Development Authority (CDA), Bureau of Internal Revenue (BIR), Government Service Insurance System (GSIS), Social Security System (SSS), Home Development Mutual Fund (HDMF) or the PAG-IBIG Fund, and Philippine Health Insurance Corporation (PhilHealth), into one platform, made available in the form of portal, mobile application, and/or other applicable variations thereof.

All other government agencies, offices, and instrumentalities, including LGUs which provide frontline services, as defined under Republic Act No. 9485, or the "Anti-Red Tape Act of 2007" as amended by Republic Act No. 11032, shall file an application for integration with the DICT. All agencies, offices, and instrumentalities that will be integrated shall establish and maintain measures to ensure that such services are accessible and capable of delivery to the public through the platform;

(b) Electronic Local Government Unit (eLGU) System. – In compliance with Section 9(g), LGUs shall establish their own portal or utilize the eLGU system developed by the DICT and its equivalent programs and systems: *Provided,* That LGUs unable to establish their own systems within one (1) year from the effectivity of this Act are mandated to utilize the eLGU or equivalent programs and systems: *Provided, further,* That LGUs establishing their own portal or those with existing portals shall immediately be connected by the DICT: *Provided, finally,* That the eLGU software or equivalent,

including its necessary infrastructure, shall likewise be provided by the DICT for the effective use of the eLGU to the unserved and underserved municipalities;

(c) Government Digital Payment Systems for Collection and Disbursement. – An electronic payment facility and gateway that will enable citizens and businesses to remit and receive payments electronically to or from government agencies shall be created. It shall render services through various delivery channels, which include debit instructions (ATM accounts), credit instructions (credit cards) and mobile wallets (mobile application/SMS). For this purpose, the government may, in accordance with applicable laws and rules, engage the services of, and interconnect with, public and private payment systems and facilities, among others, consistent with the National Retail Payment System Framework of the BSP.

These systems should smoothly interface with the current monitoring and accounting systems of the National Treasury;

(d) Government Public Key Infrastructure (PKI) Program. – The DICT shall encourage and promote the use of Government PKI digital certificates that allow paperless transactions and remote approval of signatories in the government to reduce red tape, and enforce ease of doing business. The adoption of PKI aims to strengthen E-Government security through its implementation in all government offices and supply of digital certificates to the citizens. The PKI digital certificates shall ensure the security of digital data and transactions by providing:

(1) Authentication to prevent unauthorized disclosure of information;

(2) Confidentiality to ensure that a message remains unmodified during transmission;

(3) Integrity to validate the identity of senders; and

(4) Non-repudiation to ensure non-deniability of actions by any party;

(e) Human Capital Management Information System (HCMIS). – An HCMIS shall be developed to eliminate paper-based and manual human resource (HR)-related processes. Consistent with applicable civil service laws and rules, the HCMIS shall automate the following HR-related functions in government: recruitment and selection, appointment preparation and submission, personnel records keeping, salary, benefits and payroll administration, leave management, learning and development, rewards, recognition, and performance management, among others. This system shall utilize analytics to provide insights necessary for strategic HR functions such as performance management, forecasting, promotion, succession planning, among others: *Provided,* That government agencies, offices, and instrumentalities granted by law and by their respective Charters with fiscal and administrative autonomy in the performance of their Constitutional and statutory mandates, including

those that have been exempted from the Salary Standardization Law and have been granted authority to formulate their own classification systems, shall be allowed to independently develop, maintain, undertake, supervise, and regulate their own HCMIS and shall only be required to coordinate and report to the DICT for alignment of policy objectives;

(f) Integrated Financial Management Information System (IFMIS). – To ensure fiscal discipline, fund allocation efficiency, and operational efficiency in the delivery of public services, an IFMIS shall be jointly developed by the DBM, Department of Finance, Commission on Audit, and DICT. This shall harmonize all existing financial systems in government to enable real-time, online accounting monitoring, and control of obligations and disbursements and directly link these to cash management for a more effective financial control and accountability. This shall facilitate the generation and monitoring of vital information on all aspects of

government financial transaction to support timely and informed decisions across the bureaucracy;

(g) Integrated Government Network (IGN). – An integrated, dedicated, interconnected, interoperable, secure, and resilient government network shall be established to act as the primary means for the sharing and communication of resources, information, and data through digital and electronic platforms across all agencies of government, covering all branches, agencies, instrumentalities, and offices of the national and local governments, including GOCCs.

Such network shall also act as the government's primary and focal information management tool and communications network and the data traffic that will be coursed by the government agencies and key stakeholders through this network will be exchanged through a designated Government Internet Protocol Exchange (G/IPX) facility. Interconnectivity and interoperability measures shall be established and maintained between all

existing internal networks and the IGN. This program shall also cover the acquisition and management of internet resources of the government, such as internet protocol (IP) addresses, and domain names, among others;

(h) Online Public Service Portal. – Complementing the CFDSP, an Online Public Service Portal shall be made accessible, through digital platforms, such as the internet and other ICTs, to citizens of the Philippines; foreign nationals who have been lawfully admitted to the country; and businesses organized and existing or operating under the laws and rules of the Philippines for purposes consistent with the efficient delivery of public services. The Online Public Service Portal shall serve as a helpdesk where citizens can request for information and assistance on government frontline services, service procedures, and report commendations, appreciation, complaints, and feedback.

For purposes of interoperability, interconnection, and harmonization, all existing systems or mechanisms, such

as the 8888 Citizens' Complaint Center and government social media channels, established and/or maintained by government agencies, offices, and instrumentalities, and LGUs shall be integrated to the Online Public Service Portal. Likewise, the Online Public Service Portal shall be fully integrated with the IGN and Records and Knowledge Management Information System for real time updating of data and information.

To ensure that the public is served efficiently and expeditiously in accordance with the objectives of this Act, all national government agencies, offices, and instrumentalities, GOCCs, government financial institutions, as well as the LGUs, are hereby mandated to cooperate and coordinate with the Presidential Management Staff and each other to ensure prompt action on the concerns received through the Online Public Service Portal and associated communication channels.

Notwithstanding the provisions of this Act, access to and use of resources, information, and data through the portal shall be in accordance with Republic Act No. 11032 and all relevant laws, rules, and regulations on data and information privacy and pertinent rules on confidentiality of government information;

(i) Philippine Digital Health System. – A comprehensive, integrated, interoperable, progressive, secure, and sustainable ICT system and framework shall be established to provide wide access to quality health information and services that promotes and ensures streamlined and safety-regulated delivery of digital health services to reduce inequalities and achieve universal healthcare and better health outcomes for every Filipino;

(j) Philippine Government Interoperability Framework. – A Philippine government interoperability framework shall guide and govern the basic technical and informational interoperability of government ICT systems necessary for the effective and efficient delivery of

government services. Such a framework shall provide shared operations and services of the Philippine government, between and among its various agencies, as well as for these agencies in dealing with their various constituencies. This shall be reviewed and updated regularly, to ensure responsiveness to the current needs of the government and alignment with the newly adopted standards;

(k) Procurement System. – A modernized Philippine Government Procurement System shall be developed and implemented to provide an auditable online system that encompasses all procurement and supply chain management processes involving bidding, contract management, delivery, acceptance, and payment for services or supplies: *Provided,* That government agencies, offices, and instrumentalities granted by law and by their respective Charters with fiscal and administrative autonomy in the performance of their constitutional and statutory mandates, shall independently develop, maintain, undertake, supervise,

and regulate their own procurement systems and shall only be required to coordinate and report to the DICT for alignment of policy objectives: *Provided, further,* That such system shall comply with Republic Act No. 12009, or the "New Government Procurement Reform Act"; and

(l) Records and Knowledge Management Information System. – A records and knowledge management information system shall be designed to systematically and efficiently manage government documents, records, and knowledge products and services. This includes the digitization of paper-based documents, records, and knowledge products and services, as well as the re-engineering and digitalization of paper-based workflows, from creation, dissemination, processing, analysis, tracking, storing, verification and authentication, and archiving or disposal, while adhering to existing policies, laws, and internationally recognized standards and best practices.

A repository and corresponding secure Application Programming Interfaces (APIs) shall be created for the common data sets, which include pricing data, demographic data, and geospatial data to improve publication, sharing, and utilization of data across the government. The DICT shall ensure that such repository shall be compliant with applicable data privacy laws and information security standards, in coordination with the National Privacy Commission (NPC). The DICT shall also establish a government data storage and interoperability platform or its equivalent to store all information and services that are currently housed in the government data center.

SEC. 10. *Privacy Impact Assessment (PIA).* – The DICT shall conduct a mandatory PIA, according to relevant NPC guidelines, on the proposed systems for processing personal data included in the EGMP before its publication, to identify privacy risks and establish the appropriate controls framework in line with existing data privacy and cybersecurity standards.

SEC. 11. *Minimum Information Security Standards Compliance.* – The DICT shall prescribe and implement minimum information security standards for E-Government, aligned with internationally accepted standards, relevant law, rules and regulations, including its own policies, to ensure the security of all ICT systems utilized.

The DICT is mandated to provide the proper guidance, assistance, and training on cybersecurity standards to all government agencies, offices, and instrumentalities that are part of the E-Government system. Nothing in this Act prevents a government agency, office, or instrumentality from implementing additional standards, or other standards higher than the minimum set by the DICT as it deems necessary.

SEC. 12. *Protection of Government Critical Information Infrastructure (CII).* – The DICT, in coordination with relevant government agencies and stakeholders, shall issue guidelines for the protection of

government CII identified in the EGMP. All government CIIs shall undergo Vulnerability Assessment and Penetration Testing (VAPT) before deployment and an annual risk and security assessment.

All government CII shall create an organizational Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT) and report major information security incidents affecting their institutions to the DICT's National Computer Emergency Response Team (NCERT), which shall be the central authority for all the sectoral and organizational CERTs in the country.

SEC. 13. *Public Service Continuity Plan.* – Consistent with the existing issuances of the National Disaster Risk Reduction and Management Council (NDRRMC) and CSC, all ICT systems and infrastructure covered in the priority programs of the EGMP and ISSPs shall be included as part of the Public Service Continuity Plan (PSCP) of all government agencies and instrumentalities, to ensure the

continuous delivery of essential agency functions, notwithstanding any emergency or disruption.

SEC. 14. *National E-Government Development Index (EGDI) and E-Government Maturity Survey.* – The DICT shall, in coordination with other government agencies, establish a national E-Government Development Index, which provides globally competitive indicators, definitions, and statistical standards. They shall develop a manual for measuring E-Government indicators to institutionalize the measurement framework and conduct an annual E-Government maturity survey to assess the ICT readiness and maturity of agencies, with the survey results primarily used for formulating and updating EGMP.

SEC. 15. *Free Access to the Internet for the Public.* – Subject to compliance with existing laws, rules, and regulations, the free public internet access program shall utilize the free public internet access fund (FPIAF) to provide necessary computer systems, programs, databases, management and information systems, and core

transmission and distribution networks to facilitate knowledge-building among citizens and empower them to participate in the evolving digital age.

CHAPTER IV

ROLE OF GOVERNMENT AGENCIES, OFFICES, AND INSTRUMENTALITIES

SEC. 16. *Responsibilities of the Heads of Government Agencies, Offices, and Instrumentalities.* – The head of each agency, office, or instrumentality of the national and local governments, in consultation with the DICT, shall ensure:

(a) Adherence to the requirements of this Act, including related standards for all ICT infrastructures, systems, equipment, designs, and all other technology promulgated by the DICT;

(b) Compliance with the standards and protocols for cybersecurity, resiliency, data privacy and confidentiality, promulgated by the DICT in consultation with the NPC;

(c) Prompt and effective communication of information technology standards promulgated by the DICT to all concerned agency officials;

(d) Support for the efforts of the national and local government to develop, maintain, and promote an integrated system of delivering government information and services to the public;

(e) Establishment and implementation of policies and standards on information security, freedom of information, and open data within their organization following its mandate and technological needs or risks;

(f) Conformity to the re-engineering and streamlining requirements of the Anti-Red Tape Authority (ARTA) as provided under Republic Act No. 11032;

(g) Undiminished availability of government information and services for individuals and entities who lack access to the internet; and

(h) Availability of alternative modes of delivery that make government information and services more accessible to individuals, either electronically or manually.

SEC. 17. *Chief Information Officer*. – All covered government entities under this Act shall create a plantilla position for a Chief Information Officer who shall ensure the development and implementation of the agency's ICT plan, its security and compliance with DICT-prescribed standards, relevant laws, rules, and regulations, including Republic Act No. 10173 or the "Data Privacy Act of 2012".

Recruitment, selection, and appointment to the position shall be subject to civil service laws, rules regulations, and competency standards prescribed by the DICT.

SEC. 18. *Functions of the CIO*. – The CIO shall perform the following functions:

(a) Advise agencies on how to leverage ICTs to optimize the delivery of secured public services and achieve efficient and cost-effective operations;

(b) Securely develop, maintain, and manage the agency's information systems;

(c) Manage and supervise the implementation of ICT related projects, systems, and processes;

(d) Formulate and implement processes in relation to the adoption of ICT-based solutions, including emerging technologies as provided in the EGMP;

(e) Manage operational risks related to ICT in coordination with the agency's management and stakeholders;

(f) Ensure that the ICT programs and operations are consistent with national policies and prevailing industry standards;

(g) Accelerate the adoption of open data, blockchain, and emerging technologies, while benchmarking against ICT industry best practices in ICT programs and operations;

(h) Ensure that personal information and data in government information systems are secured and protected; and

(i) Ensure that E-Government Programs are accessible and inclusive to persons with disabilities, as far as practicable.

CHAPTER V
GOVERNMENT WEBSITES AND INFORMATION PORTALS

SEC. 19. *Government Website and Electronic Bulletin (E-Bulletin) Board.* – National government agencies, offices, instrumentalities, including local governments, are mandated to consistently enhance their existing website and establish an e-Bulletin Board for efficient information dissemination. The website and e-bulletin board should be interactive, well-designed, functional, and mobile-friendly, prioritizing security and accessibility. Regular updates to website content shall also be required.

SEC. 20. *Minimum Standards.* – The following shall be the minimum standards for government websites and information portals. They shall:

(a) Include direct and easily identifiable links to: (1) description of the mission, statutory authority, and the organizational structure of the agency; and (2) frequently asked questions (FAQs) with the corresponding answers; and other common matters of public concern;

(b) Include direct and easily identifiable links to the relevant and applicable portals and E-Government programs public service delivery;

(c) Include the ability to provide access to public information via an API;

(d) Include an up-to-date government directory containing the contact information, such as emails and telephone numbers of the offices and officials within an agency;

(e) Be compliant with the Philippine Web Accessibility policy, or any relevant and updated issuance from the DICT; and

(f) Provide a real-time citizen feedback mechanism integrated into all E-government platforms to allow users to rate services, provide comments, and report issues directly. Data from this mechanism shall be publicly aggregated and published quarterly to ensure transparency and guide service improvements.

SEC. 21. *Information Dissemination Through Website and Board.* – Government offices, agencies, and instrumentalities required by law or rules to share public notices, documents, or information must publish them on their websites, e-bulletin boards, and verified official government social media accounts, in addition to traditional publication methods.

Except as provided by law, publication of notices, documents, or any other information on the website and e-bulletin board shall be construed as sufficient notice for

purposes of this Act. Date of publication shall be reckoned from the date on which the notice, document, or information was first uploaded and made accessible to the public.

CHAPTER VI
SECURITY AND PRIVACY

SEC. 22. *Data and Information Security.* – This Act limits the access and usage of ICT assets to authorized government personnel in compliance with applicable laws and regulations on data privacy and confidentiality of government information to protect them against any interference or unauthorized access that can hamper or otherwise compromise its confidentiality, integrity, and availability.

Destruction or disposal of data collected and stored by covered agencies upon fulfillment of their purpose shall be in accordance with existing laws, standards, and guidelines.

Any person who shall knowingly commit an act that compromises the security and integrity of government information systems, all networks interconnected thereto and interoperable therewith, to the detriment of the government and the public, shall incur criminal liability under applicable laws.

SEC. 23. *Responsibility of the National and Local Government.* – All agencies, offices, and instrumentalities of the national and local governments, including SUCs and GOCCs, shall be responsible for:

(a) Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(b) Determining the levels of information security appropriate to protect such information and information systems, and implementing the same in coordination with the DICT;

(c) Periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

(d) Ensuring procedures, standards, and guidelines, including information security standards promulgated by the DICT and information security standards and guidelines for national security systems issued in accordance with law and as directed by the President of the Philippines;

(e) Ensuring that information security management processes are integrated with agency strategic and operational planning processes; and

(f) Adopting the Privacy-by-Design, Privacy Engineering, and Privacy-by-Default principles in developing, implementing, and deploying systems,

processes, software applications, and services throughout the processing of personal data.

SEC. 24. *Master Data Management.* – In order to have access to the most updated data, the government shall establish and maintain measures to ensure that the parent government agency responsible for a set of data shall own, maintain, update, and protect the data while giving access via secure API to other agencies.

CHAPTER VII
PARTICIPATION OF THE PRIVATE SECTOR

SEC. 25. *Government Cooperation with the Private Sector.* – Nothing in this Act shall prevent the national and local governments from entering into contracts, agreements, or partnerships with the private sector to provide various resources, assets, and services to comply or enhance compliance with the provisions of this Act.

Any and all contracts or agreements with the private sector within the context of this Act shall be subject to the

laws and rules on public accountability, transparency and good governance.

To ensure inclusivity, public telecommunications entities (PTEs) and non-PTE internet service providers (ISPs) shall be allowed to enter into contracts with government agencies at the national and local levels to build and operate networks to provide internet connections in support of E-Government programs, especially in the underserved and unserved areas.

CHAPTER VIII
E-GOVERNANCE ACADEMY

SEC. 26. *Establishment of the E-Governance Academy; Purposes.* – The DICT shall reorganize and restructure its ICT Literacy and Competency Development Bureau in order to establish and develop rules and policies for the operations of an ICT Academy, herein after referred to as the "Academy" that shall have the following purposes:

(a) Become the National Center of Excellence for ICT Education;

(b) Promote education to enhance the nation's labor capacity in relation to the most relevant and updated data on local and international skills supply and demand;

(c) Promote, foster, and conduct quality ICT education for the capacity development of all citizens;

(d) Foster and support the strategic goals of the national ICT development agenda, as provided in Republic Act No. 10844 through data collection and globally competitive ICT skills development programs and for other purposes;

(e) Conduct programs and activities for the capacity development of all citizens to gain globally competitive skills and drive inclusive economic growth;

(f) Create and foster partnerships with different persons, entities, and institutions for purposes of developing and updating the Academy's resources, its ICT curriculum, modules, and pedagogical approaches;

(g) Promote gender parity through technology education;

(h) Ensure continuous learning and development of educators on current ICT trends;

(i) Promote immersion of learners to industry partners, whether in the private or public sector;

(j) Establish and implement a scholarship system for qualified individuals in training and programs under the Academy or other activities approved by the DICT Secretary;

(k) Facilitate the screening, admission process, and monitoring of all admitted scholars;

(l) Spearhead academic research and development related to ICT;

(m) Regularly assess the state of the country in terms of comparative ICT skills and performance and suggest responsive policies to address concerns; and

(n) Develop curricula and courses for learners and students on ICT to upskill ICT proficiency and competency, in collaboration with the Department of Education (DepEd), Commission on Higher Education (CHED), Technical and Skills Development Authority (TESDA), SUCs, and local universities and colleges.

SEC. 27. *Satellite Units.* – The Academy may establish satellite units in existing DICT offices in particular regions, provinces, or municipalities. To ensure broader access to quality ICT trainings and skills development and further enhance the capability of the Academy to attain its purposes, additional satellite units may be established upon determination of the DICT and in coordination with the CHED and the TESDA.

SEC. 28. *Access and Admission.* – The Academy shall be accessible to all citizens regardless of skill, age, gender, religious belief, economic status, ethnicity, physical disability, political opinion, or affiliation.

The DICT, through the Academy, shall promulgate an equitable and inclusive admission process to ensure that citizens have equal access to ICT education and that the broadest base of the citizenry shall have ICT education.

SEC. 29. *Finances.* – The operations of the Academy shall be financially supported by a budget from the DICT, reasonable fees and dues collected, as well as through donations, in accordance with applicable laws and rules.

Donations collected shall be held in a fund, to be administered in trust by a Committee created by the DICT for such purpose. The fund shall in no case be impaired. Donations received shall be used only for the purposes for which they were donated, subject to accounting and auditing rules and regulations.

SEC. 30. *Partnerships.* – The Academy may form partnerships with different educational institutions, technical and standards organizations, and private entities for purposes of achieving the goals of the Academy.

Partnerships may be in the form of research collaborations, resource sharing, module and training development, faculty exchange standards development, training collaborations, internships, apprenticeships, and other similar forms.

All partnerships entered into by the Academy shall be in accordance with the provisions of this law and approved by the DICT Secretary. There shall be no disbursement of any funds by the Academy or the government for the purpose of establishing these partnerships.

The Academy shall be empowered to accredit courses offered by educational institutions, private or public, following strict competency standards and guidelines developed by the DICT.

CHAPTER IX
MISCELLANEOUS AND FINAL PROVISIONS

SEC. 31. *Transitory Provision.* – The DICT, in consultation with relevant government agencies,

instrumentalities, private stakeholders, and civic organizations, shall study, formulate, and implement a plan for the transition to E-Government following the objectives of this Act.

Until such time that the government shall have completed the transition, all government activities covered under this Act shall be conducted in the manner provided for under existing laws and rules.

The government shall complete the transition within a period of three (3) years from the effectivity of this Act.

SEC. 32. *E-Government Interoperability Fund (EIF).* – An EIF is hereby created as a special account in the general fund managed by the DICT for the implementation of the EGP, E-Government Programs and Government Websites, including eLGU system, among others.

The EIF will be primarily sourced from donations and fees as well as Spectrum User's Fees which currently accrue to the FPIAF created under Republic Act No. 10929 or the "Free Internet Access in Public Places Act". The EIF

may be funded through grants and loans from development and foreign partners, or through applicable Public-Private Partnership mechanisms.

SEC. 33. *Appropriations.* – The amount necessary for the initial implementation of this Act on the national government level shall be charged against the current year's appropriations of the DICT, National Telecommunications Commission (NTC), NPC, or the concerned national government agency, office, or instrumentality. Thereafter, such sums needed for its continued implementation shall be included in the annual General Appropriations Act.

The amounts necessary to implement this Act on the local government level shall be charged against the funds of the LGU concerned.

SEC. 34. *Applicability of Republic Act No. 8349, as Amended by Republic Act No. 11312 and Republic Act No. 10929.* – All ICT employees across all government agencies and instrumentalities providing technical support to the

implementation of all E-Government Programs in their respective agencies shall be covered by Republic Act No. 8439, or the "Magna Carta for Scientists, Engineers, Researchers and other Science and Technology Personnel in the Government," as amended.

The provisions of R.A. No. 10929 or the "Free Internet Access in Public Places Act" shall apply suppletorily to this Act.

SEC. 35. *Implementing Rules and Regulations.* – Within one hundred eighty (180) days from the effectivity of this Act, the DICT, in coordination with relevant offices, agencies, and instrumentalities of the national and local government, shall promulgate the necessary rules and regulations in effectively implementing the law.

SEC. 36. *Regular Status Reports.* – All agencies, offices, and instrumentalities of the national and local governments shall submit an annual report on the status of implementation of this Act to the President, both Houses of Congress, and the DICT,. These reports shall be made

publicly available in government websites and information portals.

The status report shall include the following:

(a) Status of the implementation of E-Government Initiatives based on its approved ICT Plan;

(b) Compliance by the agency with this Act; and

(c) Performance in delivering programs and services through the E-Government to their constituencies.

SEC. 37. *Joint Congressional Oversight Committee on E-Governance.* – A Joint Congressional Oversight Committee on E-Governance (JCOCEG) shall be constituted to monitor and ensure the effective implementation of this Act, identify the deficiencies, limitations, and challenges in the current legal framework, and propose necessary amendments or supplementary legislation to address them.

The JCOCEG shall be composed of three (3) members from the Senate and three (3) members from the House of Representatives, in addition to the Chairperson of the

Senate Committee on Science and Technology and the Chairperson of the House of Representatives Committee on Information and Communications Technology who shall jointly chair the JCOCEG.

The minority in the Senate and the House of Representatives shall each have at least one (1) seat in the JCOCEG as Co-Vice Chairpersons.

The Secretariat of the JCOCEG shall come from the existing Secretariat personnel of the Committee on Science and Technology of the Senate and the Committee on Information and Communications Technology of the House of Representatives.

The JCOCEG shall conduct a hearing at least once every quarter to review the implementation of this Act and identify other necessary legislation.

The JCOCEG shall cease to exist after five (5) years from the effectivity of this Act.

SEC. 38. *Separability Clause.* – If any provision of this Act is declared unconstitutional, the remainder thereof not otherwise affected shall remain in full force and effect.

SEC. 39. *Repealing Clause.* – All laws, presidential decrees, executive orders, letters of instruction, proclamations, or administrative regulations that are inconsistent with the provisions of this Act are hereby repealed, amended, or modified accordingly.

SEC. 40. *Effectivity.* – This Act shall take effect after fifteen (15) days following its complete publication in the *Official Gazette* or a newspaper of general circulation.

Approved,