REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

DEPARTMENT CIRCULAR NO. 003

OCT 22 2024

Series of 2024

SUBJECT : PRESCRIBING POLICIES AND GUIDELINES ON THE CYBERSECURITY PROTECTION OF GOVERNMENT DIGITAL ASSETS STIPULATED IN THE NATIONAL CYBERSECURITY PLAN 2023-2028

WHEREAS, Article II, Section 24 of the 1987 Philippine Constitution provides that "The state recognizes the vital role of communication and information in nation-building."

WHEREAS, under Section 2 (m) of Republic Act (RA) 10844, or the Department of Information and Communications Technology (DICT) Act of 2015, it is a declared policy of the State "to ensure the security of critical ICT infrastructures including information assets of the government, individuals and businesses."

WHEREAS, under Section 5 of RA 10844, it is declared that the DICT "shall be the primary policy, planning, coordinating, implementing, and administrative entity of the Executive Branch of the government that will plan, develop, and promote the national ICT development agenda."

WHEREAS, under Section 6 of RA 10844, the DICT is mandated to "formulate, recommend and implement national policies, plans, programs, and guidelines that will promote the development and use of ICT with due consideration to the advantages of convergence and emerging technologies"; and to "assist and provide technical expertise to government agencies in the development of guidelines in the enforcement and administration of laws, standards, rules, and regulations governing ICT."

WHEREAS, Executive Order No. 58 s.2024 adopted the National Cybersecurity Plan (NCSP) 2023-2028 as the whole-of-nation roadmap for the integrated development and strategic direction of the country's cybersecurity. Under Outcome 3, 3.6 (5) of the NCSP 2023-2028, the DICT is mandated to "circularize a security-by-design and privacy-by-design frameworks that should be uniformly applied by all government agencies."

NOW, THEREFORE, pursuant to public interest, the public consultations conducted by the DICT in August and September 2024, and the provisions of existing laws, rules, and regulations, this Circular is hereby issued, adopted, and promulgated.

Section 1. Definition of Terms — As used in this Circular, the following terms shall be defined as follows:

a. **Common Vulnerability Scoring System (CVSS)** is a method used to supply a qualitative measure of severity of vulnerabilities discovered on one's systems and as a factor in prioritization of vulnerability remediation activities.

b. **Cybersecurity Incident** refers to a single or series of unwanted or unexpected information security (cybersecurity) events that have a significant probability of compromising business operations and threatening information security (cybersecurity).

c. **Domain Name System (DNS)** refers to the naming database that locates and translates internet domain names into IP addresses.

d. **Information security** refers to protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

e. **Information security incident** refers to an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

f. **Information services** refer to services that offer the capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information or data, the networks for which may be established and propagated via several devices or any one or a combination of several high-speed transmission technologies over one or more transmission mediums.

g. **Information system** refers to applications, services, information technology assets, or any component handling information.

h. **National Computer Emergency Response Team (NCERT)** refers to the division of the Cybersecurity Bureau of the DICT responsible for handling cybersecurity incident response, cybersecurity incident investigation, government VAPT services, and conducting baseline assessment of government agencies' cybersecurity posture.

i. **National Security Operations Center (NSOC)** refers to the facility of the DICT Cybersecurity Bureau that monitors systems and networks for malicious behavior and for indications of a potential cyber-attack.

j. **Vulnerability Assessment** refers to the systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Section 2. Coverage — This Circular covers all national government agencies and instrumentalities under the Executive Branch, including Government-Owned and -Controlled Corporations (GOCCs) and their subsidiaries, Government Financial Institutions (GFIs), Local Government Units (LGUs), and State Universities and Colleges (SUCs).

The Philippine Congress, the Judiciary, the Constitutional Commissions, and the Office of the Ombudsman are highly encouraged to adopt this policy.

Section 3. Establishment of Government Computer Emergency Response Team (GCERT) — All covered agencies and institutions shall establish their own GCERT dedicated to coordinate information and cyber security incidents for their respective agencies. Each GCERT is tasked to respond to cybersecurity incidents, regardless of their complexity or criticality, and coordinate with the NCERT and/or their respective Sectoral CERT (SCERT) in cases of cyber incidents.

a. Each GCERT shall be responsible for the following:
    i. **Identification**. Triage and classify cybersecurity incidents within the organization.
    ii. **Containment and Analysis**. Respond to cybersecurity incidents within the agency/institution.
    iii. **Eradication.** For severe or critical cybersecurity incidents, coordinate the response with the NCERT.
    iv. **Recovery and Learning.** Develop and manage the cybersecurity response life cycle within the organization.
    v. **Exercises.** Conduct cybersecurity tabletop simulations, drills, and exercises within the organization.
    vi. **Promotion of a cybersecurity culture**. Promote and train the organization in adopting a cyber-safe culture.
    vii. **Focal.** Appoint at least a mid-level manager as the primary focal person of the organization to the nationwide network of CERT.

b. The GCERT shall have at least three (3) personnel, preferably with a Chief Information Security Officer (CISO) position or equivalent that perform decision-making or management functions and information security officers, with sufficient cybersecurity trainings and credentials. The CISO or its equivalent shall be the point person for: (i) the development and maintenance of the agency's Information Systems Strategic Plan (ISSP) relevant to cybersecurity; (ii) compliance with prescribed cybersecurity standards; (iii) building information security capability within the agency; and (iv) compliance with the agency's reporting requirements.

c. The composition of GCERT may vary depending on the need and available resources of the agency or institution. However, the team must be regularly upskilled in defensive security and incident management.

Section 4. Mandatory Connection to DICT-managed PDNS — All covered agencies and institutions shall connect their internet traffic to the DICT-managed Protective Domain Name System (PDNS). This mandatory connection aims to:

a. **Enhance national cybersecurity posture.** By utilizing a centralized PDNS solution managed by the DICT, government agencies benefit from a consistent and robust security layer.

b. **Improve threat intelligence and protection.** DICT can leverage its resources and expertise to maintain a comprehensive threat intelligence feed, ensuring all connected institutions benefit from the latest security updates and domain filtering.

c. **Simplify management and reduce costs.** The centralized PDNS eliminates the need for individual agencies to manage and maintain their own PDNS solutions, potentially reducing overall cybersecurity expenditures.

In connecting to the DICT-managed PDNS, all covered agencies and institutions shall have an IP address management system integrated within their operations and may choose one of the following options:

(1) ISPs to point and configure their recursive DNS to DICT's protective DNS.
(2) Receive an automated threat feed of sites to block from the DICT's PDNS and to configure their respective DNS automatically.
(3) Configure their DHCP settings to align with the DICT PDNS.

The DICT Cybersecurity Bureau shall issue additional guidelines and procedures to connect to the DICT-managed PDNS. Technical specifications and configuration details for connecting to the PDNS will be provided in a separate technical advisory.

Section 5. Project Secure Online Network Assessment and Response System (SONAR) Implementation — The DICT conducts vulnerability scanning and detection across various government agencies and instrumentalities to monitor and mitigate risks associated with identified flaws and misconfigurations of publicly accessible digital assets of government agencies and instrumentalities through Project SONAR.

A. **Mandatory Participation.** All covered agencies and institutions are required to participate in Project SONAR. The DICT shall inform the concerned institution of the conduct of automatic scanning one day before its schedule.

B. **Vulnerability Reporting.** DICT shall provide participating agencies and institutions with regular reports detailing identified vulnerabilities and their severity levels or their CVSS.

C. **Vulnerability Remediation.** Each covered agency and institution is responsible for prioritizing and remediating identified vulnerabilities based on their severity and potential impact. DICT shall provide technical assistance and guidance for vulnerability remediation.

D. **Automation.** DICT shall establish a dedicated online portal for vulnerability reporting and remediation status updates of covered institutions.

E. **Reporting Requirements for Government ICT Systems.**

a. Communication from the DICT to Government ICT System Owners
   i. DICT shall provide a summary of detected vulnerabilities in publicly accessible ICT systems owned by the government.
   ii. Recommendations for mitigating identified vulnerabilities in the government ICT system owner's assets shall be included.
   iii. The rationale behind conducting vulnerability assessments must be clearly outlined.

b. Monthly Cybersecurity Baseline Report Submission
   i. DICT shall submit a monthly report detailing baseline cybersecurity scores that must be meticulously prepared and submitted to the National Cybersecurity Inter-Agency Committee (NCIAC) and the Office of the President.
   ii. The report shall encompass comprehensive assessments of the cybersecurity posture highlighting significant incidents or anomalies.
   iii. Recipients of the report are required to review its contents and provide feedback to facilitate continuous improvement in cybersecurity measures.
   iv. Strict adherence to confidentiality and compliance requirements is mandatory to ensure that sensitive information is safeguarded and shared only with authorized personnel.

F. **Monthly Scanning.** Following the establishment of reporting requirements, the DICT shall conduct monthly automated vulnerability scanning and detection processes across all publicly accessible government ICT systems.

Section 6. National Security Operations Center — All covered agencies and institutions shall connect to the National Security Operations Center (NSOC) managed by the DICT by submitting a letter of intent duly signed by the head of agency or institution. Details on the connection process shall be provided by the DICT once the signed letter of intent is received.

Section 7. Traffic Light Protocol — All covered agencies and institutions shall comply with established communication protocol, using at the minimum the Traffic Light Protocol for information sharing, to ensure that information is only shared on the desired and appropriate audience or recipient.

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most

		circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organization.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organization involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
TLP:GREEN Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Section 8. Incident Reporting — All covered agencies and institutions are required to report any security incidents or suspected breaches following the prescribed process issued by the DICT. Non-compliance resulting in a security incident shall be subject to the provisions of relevant laws, rules and regulations including but not limited to RA 10175 otherwise known as the Cybercrime Prevention Act of 2012.

Section 9. Funding — The funding requirements for the implementation of this Circular shall be charged against the existing budget of the covered agency or institution, and such other appropriate funding sources as the Department of Budget and Management (DBM) may identify, subject to relevant laws, rules, and regulations.

Section 10. Separability Clause — If any part, section, or provision of this Circular is declared invalid or unconstitutional, the remaining provisions not affected thereby shall continue to be in full force and effect.

Section 11. Repealing Clause — All other circulars, departmental issues, or parts thereof that are inconsistent with this Circular are hereby amended, modified, repealed, or superseded or modified accordingly.

Section 12. Effectivity Clause — This Circular shall take effect fifteen (15) calendar days after its publication in the Official Gazette or any newspaper of general circulation and upon filing with the Office of the National Administrative Register (ONAR) of the University of the Philippines Law Center.

Let copies of this Circular be posted and published on the official DICT website and bulletin boards.

IVAN JOHN E. UY
Secretary

PRESCRIBING POLICIES AND GUIDELINES ON THE CYBERSECURITY PROTECTION OF GOVERNMENT DIGITAL ASSETS STIPULATED IN THE NATIONAL CYBERSECURITY PLAN 2023-2028