REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

DEPARTMENT CIRCULAR NO. 005
Series of 2024

OCT 22 2024

SUBJECT : REPORTING MECHANISMS AND MANDATORY DISCLOSURE OF CYBERSECURITY INCIDENTS FOR THE GOVERNMENT

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

WHEREAS, under Section 2 (n) 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 provide oversight over agencies governing and regulating the ICT sector and ensure consumer protection and welfare, data privacy and security, foster competition and the growth of the ICT sector."

WHEREAS, under Section 5 of RA 10844, the DICT is the "primary policy, planning, coordinating, implementing, and administrative entity of the Executive Branch of the government that will plan, develop, and promote the national Information and Communications Technology (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, cyber incidents encountered by the public sector are becoming more prevalent and sophisticated, making the cybersecurity of government information infrastructure an urgent priority.

WHEREAS, public institutions serve as custodians of vital information from both the state and citizens and are therefore imbued with public interest. Statistics from January 2022 to August 2024 show that government and emergency services remain to be the top-targeted sectors of cyber-attacks. Thus, securing the information infrastructure of government agencies has become an immediate priority against cyber threats.

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.

WHEREAS, under Outcome 3.7.1 of the NCSP 2023-2028, incidents classified as severe or critical shall be reported to National Computer Emergency Response Team (NCERT) and Sectoral Computer Emergency Response Teams (SCERT) to ensure proper management of incidents at a sectoral and national scale.

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. Purpose — This Circular aims to develop and implement effective mechanisms for the Government in terms of reporting and disclosing cybersecurity incidents, to mitigate risks, facilitate coordinated responses, and to comply with regulatory requirements ensuring timely and transparent communication of cybersecurity incidents.

Section 2. Coverage — This Circular shall apply to 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 Independent Constitutional Commissions, and the Office of the Ombudsman, are highly encouraged to adopt this Circular.

Section 3. Reporting Mechanism — All covered agencies and institutions shall adopt and implement adequate mechanisms for cybersecurity breaches, in compliance with existing laws, rules, and regulations, as follows:

a. **Establish a Governance Structure** – Set up governance structure to oversee the development, implementation, and enforcement of incident reporting and disclosure policies.

b. **Develop an Incident Response Manual** – Create an Incident Response Manual for the mitigation of cyber incidents within their organization and develop a communication plan for informing internal stakeholders, including management, employees, and contractors, about cybersecurity incidents, in accordance with Section 6 of this Circular.

c. **Develop a Reporting Mechanism** – Establish a reporting mechanism to the NCERT and include it in the Incident Response Manual, following the guidelines provided by NCERT for cyber incident reporting.

d. **Ensure Compliance by Third-party Service Providers** – Ensure that outsourced cybersecurity and information services adopt national and international standards

pertaining to the protection and security of government data against cyber-attacks and breaches. In the event of a breach of government data, the concerned government agency/institution shall be held liable under the pertinent provisions of applicable laws, rules, regulations, and other relevant issuances.

e. **Provision of Training** – Provide regular training for employees on recognizing and reporting cybersecurity incidents.

Section 4. Coordinating Computer Emergency Response Teams (CERTs) — The following are the Computer Emergency Response Teams (CERTs) interoperating in responding to cybersecurity incidents during computer emergencies:

a. The **NCERT or CERT-PH** serves as the Central Authority for all CERTs to coordinate information sharing and incident response services through the various organization CERTs. As a coordinating CERT, the CERT-PH will conduct training and exercises to various CERTs and define the framework and procedures to resolve cybersecurity incidents.

b. The **Sectoral CERT or SCERT** is a coordinating CERT for critical information infrastructures (CIIs), created for administrative and/or regulatory agencies that oversee the operations of CIIs.

c. The **Government CERTs (GCERT)** are government computer emergency response teams dedicated to coordinating information and cyber security incidents for their respective agencies. The GCERT is tasked to respond to cybersecurity incidents, regardless of their complexity or criticality, while the NCERT or SCERT will provide specialist support and information to the GCERT.

Section 5. Mandatory Disclosure of Cybersecurity Incidents — All covered agencies and institutions shall:

a. Report all detected material cybersecurity incidents to the CERT-PH, and to the Sectoral CERT if applicable, using its prescribed reporting template, or any available secure means for the swift transfer of information;

b. Submit a cybersecurity incident detection report to the CERT-PH, and to the Sectoral CERT, if applicable, depending on the following threat levels of the cybersecurity incident:

Color Indicator	Threat Level	Report to	Description	Report Timeframe
Yellow	Elevated	CERT-PH and Sectoral CERT	Detected known vulnerabilities, Idle botnets and backdoors , Unresolved signs of system intrusion(website defacements, etc.)	24 hours upon discovery of the incident
Orange	High	CERT-PH and Sectoral CERT	Compromised executive email, Malware infiltration, Network and system Intrusion	18 hours upon discovery of the incident
Red	Critical	CERT-PH and Sectoral CERT	Ransomware, C&C Server, DDOS affecting all critical sectors, Data breach with CIIs exposed, wide-spread destructive compromised system, zero-day, Supply Chain attacks	12 hours upon discovery of the incident

i. Cybersecurity incidents with Elevated threat level shall be reported to the CERT-PH and the Sectoral CERT within 24 hours upon the discovery of the incident;
ii. Cybersecurity incidents with High threat level shall be reported to the CERT-PH and the Sectoral CERT within 18 hours upon the discovery of the incident;
iii. Cybersecurity incidents with Critical threat level shall be reported to the CERT-PH and the Sectoral CERT within 12 hours upon the discovery of the incident.

c. The report shall contain basic information about the cybersecurity incident, such as:
   i. name of the authorized person to submit the report;
   ii. date when the incident was first detected;
   iii. nature of the information security incident;

iv. possible business processes and functions compromised;
v. agency's initial response and next steps; and
vi. risk assessment.

d. Submit an incident progress report, upon request of the CERT-PH, in order to help assess and provide the necessary support in responding to the cybersecurity incident;

e. Submit a post-incident report, which contains the following information:
   i. the magnitude of business operations compromised;
   ii. the agency's response; and
   iii. mitigation strategy.

   They shall also provide the necessary additional information about the cybersecurity incident, as requested by the CERT-PH;

f. Compile on an annual basis a summary of all information security incident reports and submit an annual report to the DICT Cybersecurity Bureau every 31st of March;

g. Comply with the reporting mechanism and template prescribed by the DICT in the submission of all the reporting requirements described above; and

h. Follow the prescribed threat level indicators of the CERT-PH for the criticality level of cybersecurity incidents.

Section 6. National Incident Response Manual – The CERT-PH shall issue the National Incident Response Manual that details the cybersecurity incident reporting mechanism in Section 5 of this Circular to all cover agencies and institutions. The National Incident Response Manual establishes the roles, responsibilities, and communication procedures for the CERT-PH and different stakeholders when responding to cybersecurity incidents and sharing of threat information.

Section 7. Information Sharing Protocol — The sensitivity of information communicated during the process of cybersecurity incident reporting shall be carefully considered by the DICT at all times. Information sharing shall be done with the use of established communication protocol to ensure that information is shared only with the appropriate audience or recipient. At the minimum, the Traffic Light Protocol (TLP) as prescribed by the DICT shall be used.

Section 8. Funding — The initial funding requirements for the implementation of this Circular shall be charged against the existing budget of the covered agencies and institutions and such other appropriate funding sources as the Department of Budget and Management (DBM) may identify, subject to relevant laws, rules, and regulations.

Section 9. Penalty — 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 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 — DICT Memorandum Circular No. 005, s.2017 is hereby amended. All other circulars, departmental issues, or parts thereof that are inconsistent with this Circular are hereby amended, modified, repealed, or superseded 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

REPORTING MECHANISMS AND MANDATORY DISCLOSURE OF CYBERSECURITY INCIDENTS FOR THE GOVERNMENT