RECEIVING COPY
CRRU-O-2024-10-296
U.P. LAW CENTER
OFFICE of the NATIONAL ADMINISTRATIVE REGISTER
Administrative Rules and Regulations
OCT 29 2024
REGISTERED
ONAR Registration
TIME: BY:

REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

DEPARTMENT CIRCULAR NO. 006
Series of 2024

OCT 22 2024

SUBJECT : GUIDELINES FOR THE VULNERABILITY DISCLOSURE INITIATIVE

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, 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 or the Department of Information and Communications Technology Act of 2015, 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, Executive Order No. 58 s.2024, the National Cybersecurity Plan (NCSP) 2023-2028 is "adopted as the whole-of-nation roadmap for the integrated development and strategic direction of the country's cybersecurity."

WHEREAS, 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." Under 3.7.2 of the NCSP 2023-2028, the DICT seeks to create a safe environment for security researchers to responsibly disclose cybersecurity incidents.

WHEREAS, the protection of government agencies from cyber-attacks, data manipulation, and other cybercrimes is a matter of national security. Addressing current and future cybersecurity threats calls for a whole-of-nation approach where the assistance of well-meaning researchers should be welcomed and not discouraged.

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. Vulnerability Disclosure Initiative — This initiative aims to create a safe environment for security researchers to responsibly disclose cybersecurity vulnerabilities and incidents. This Circular details the guidelines for responsible disclosure of government vulnerabilities.[1]

[1] National Cybersecurity Plan 2023-2028, p. 28

Department of Information and Communications Technology (DICT)
General Services Division
Records and Archives Management Section
CERTIFIED TRUE COPY
CHERRY RABULAN-JACOB
Administrative Officer V (Records Officer III)
Date: 28 OCT 2024

Section 2. Coverage — This Circular shall apply to the following persons, entities, and/or organizations:

2.1 All National Government Agencies 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).

2.2 Vulnerability reporters responsible for identifying and analyzing potential threats to an organization's network and systems;

The Philippine Congress, the Judiciary, the Independent Constitutional Commissions, and the Office of the Ombudsman are highly encouraged to adopt this Circular. The private sector is strongly encouraged to develop their own bug bounty/vulnerability disclosure programs.

Section 3. Definition of terms — As used in this Circular, the following terms shall be defined as follows:

a. The **National Institute of Standards and Technology - National Vulnerability Database (NIST-NVD)** is the U.S. Government repository of standards-based vulnerability management data, enabling automation of vulnerability management, security measurement, and compliance (e.g., FISMA).[2]

b. **Vulnerability** is a weakness of an asset or control that can be exploited by one or more threats.[3]

c. **Vulnerability reporter** is any person that reports a vulnerability to the Government that may be outside of the Government, within the Government, or within the specific system that has the vulnerability.[4]

Section 4. Requirements for the participation and submission of reports — Vulnerability reporters may submit their reports through a reporting platform developed by the DICT. To participate in this program, the vulnerability reporter shall disclose the following information:

a. real name;
b. validated e-mail address;
c. validated phone number; and
d. pseudonym, if applicable.

Section 5. Determination of a valid report — The submission of a vulnerability reporter should include the full description of the vulnerability and the name of the Agency/Organization where the vulnerability was discovered, along with its affected ICT asset, including the following information as much as possible:

---

[2] NIST-NVD as defined by https://csrc.nist.gov/glossary/term/national_vulnerability_database
[3] National Cybersecurity Plan 2023-2028, p. xiii
[4] Reporter as defined by https://csrc.nist.gov/glossary/term/reporter

Department of Information and Communications Technology (DICT)
General Services Division
Records and Archives Management Section
CERTIFIED TRUE COPY
CHERRY RABULAN-JACOB
Administrative Officer V (Records Officer III)
Date: 28 OCT 2024

a. Type of vulnerability (ex. SQL injection, cross-site scripting, buffer overflow, etc);
b. Description of the potential impact of the vulnerability, and how an attacker could exploit it;
c. All steps required to reproduce the exploit of the vulnerability;
d. Proof of concept or exploit code;
e. Saved attack logs; and
f. URLs and/or applications affected.

The type of vulnerability will be based on the categories as enumerated in the National Institute of Standards and Technology - National Vulnerability Database (NIST-NVD) at https://nvd.nist.gov/vuln/categories. Insufficiency of data and the intricacy of a vulnerability report may impact the duration of its review, as well as the decision to grant recognition.

In the event that the vulnerability is reported by two or more vulnerability reporters, the earliest reporter shall be officially recognized, subject to proper validation.

Section 6. Responsibilities of the Vulnerability Reporter — The Vulnerability Reporter shall have the following responsibilities:

a. Officially register through the reporting platform before performing any action in relation to this Circular. By registering, the Vulnerability Reporter agrees to the terms and conditions of the program;

b. Only participate in the Program solely for the intended purpose of disclosing vulnerabilities to the DICT as described in this Circular;

c. Participate in the Program for lawful purposes only, and shall comply with all applicable laws, rules, and regulations;

d. Only access, disclose, or modify their own data and be solely responsible for the accuracy, completeness, appropriateness, and legality of any data or vulnerabilities they upload and/or provide through their participation in the Program;

e. Keep the confidentiality of the reported vulnerability in accordance with this Circular and not disclose to any third-party data and/or information accessed and/or obtained through or in connection with their participation in the program or through the process of discovering such vulnerabilities for at least ninety (90) days.

Section 7. Prohibited Actions for the Vulnerability Reporter — The Vulnerability Reporter shall be prohibited from performing the following:

a. Use scanning, denial of service, spamming and related techniques and/or attacks, which may harm, cause degradation of, or otherwise influence the integrity or reliability of the ICT assets of the system owner.

Department of Information and Communications Technology (DICT)
General Services Division
Records and Archives Management Section
CERTIFIED TRUE COPY
CHERRY RABULAN-JACOB
Administrative Officer V (Records Officer III)
Date: 28 OCT 2024

b. Transmit any viruses or exploits through the Vulnerability Reporter's use of the program, except for the sole purpose of discovery and submission of vulnerabilities and subject to compliance within this Circular.

c. Encrypt any data found on the ICT assets of system owners. Exceptions to this rule shall be determined by the DICT on a case-to-case basis provided that the Vulnerability Reporter provides:
   i. a justifiable explanation for encrypting data;
   ii. the decryption key.

d. Exfiltrate data. Data exfiltration may result in immediate termination of the Vulnerability Reporter's participation in the program, blacklisting, and possible legal action/s. However, if said data exfiltration forms part of or essential to testing the alleged vulnerability, the Vulnerability Reporter agrees to:
   i. Keep the data confidential;
   ii. Absolute deletion of the data copied after the submission of a report;
   iii. Screenshots may be kept as long as properly redacted for any sensitive information or personally identifiable information.

e. Disclose any suspected vulnerability to any third party before it is resolved. Malicious actors could exploit the vulnerability, potentially causing damage, harm, or loss to individuals and organizations.

The DICT reserves the right, without liability or prejudice to other rights, to disable a Vulnerability Reporter's access to this program at any time, or if the Vulnerability Reporter is found in breach of obligations as enumerated in this Circular. A Vulnerability Reporter may file an appeal with the Cybersecurity Bureau Director of the DICT within thirty (30) days from notice of suspension or removal from the program. The Cybersecurity Bureau Director shall decide on the appeal within thirty (30) days of receipt of the appeal.

Section 8. Responsibilities of the Cybersecurity Bureau — The Cybersecurity Bureau, shall perform the following functions to implement this Circular:

a. Serve as a liaison between the Vulnerability Reporter and the relevant public sector agency or agencies that may be affected by the suspected vulnerability;

b. Confirm receipt of the suspected vulnerability report and notify the stakeholders of the said vulnerability within five (5) business days of receiving the report;

c. Collaborate with the vulnerability reporter and the stakeholders to resolve any validated vulnerability within 90 business days of receiving your report.

d. Upon validating a suspected vulnerability report, and at DICT's sole discretion, provide appropriate recognition for the Vulnerability Reporter's contribution in reporting and/or resolving the validated vulnerability.

Department of Information and Communications Technology (DICT)
General Services Division
Records and Archives Management Section
CERTIFIED TRUE COPY
CHERRY RABULAN-JACOB
Administrative Officer V (Records Officer III)
Date: 08 OCT 2024

Section 9. Recognition of Vulnerability Reporter — There shall be no monetary reward for this program in the public sector. Validated reports shall be attributed to the Vulnerability Reporters in a recognition page in the DICT official website. Vulnerability Reporters may appeal possible misattributed contributions within thirty (30) days of posting on the official recognition page.

Section 10. Confidentiality — The DICT shall uphold the confidentiality of received reports, subject to relevant provisions of the Data Privacy Act. Only the provided pseudonym of the vulnerability reporter shall be published unless the latter gives his/her consent.

Section 11. Monitoring and Reporting — A monthly report shall be prepared by the DICT Cybersecurity Bureau that will be submitted by the DICT to the Chairpersons of the National Cybersecurity Inter-Agency Committee (NCIAC) and to the Office of the President.

Section 12. Funding — The initial funding requirements for the implementation of this Circular shall be charged against the existing budget of the covered public institution and such other appropriate funding sources as the DBM may identify, subject to relevant laws, rules, and regulations.

Section 13. 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 14. 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 15. 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

GUIDELINES FOR THE VULNERABILITY DISCLOSURE INITIATIVE

Department of Information and Communications Technology (DICT)
General Services Division
Records and Archives Management Section
CERTIFIED TRUE COPY
CHERRY RABULAN-JACOB
Administrative Officer V (Records Officer III)
Date: 28 OCT 2024