Comments to and Recommendations for the Philippine National Cybersecurity Plan 2023-2028

July 25, 2023

Atty. Ivan John E. Uy
Secretary
Department of Information and Communications Technology (DICT)
Philippines

Thru:Office of the Assistant Secretary for Cybersecurity and Upskilling, and the Cybersecurity Bureau

Dear Atty. Uy,

Access Now respectfully submits our comments and recommendations to the Draft National Cybersecurity Plan 2023-2028. We thank you for the opportunity to participate in this process.

We look forward to continuous engagement with the Department of Information and Communications Technology (DICT).

Sincerely,

Atty. Golda Benjamin
Campaigner for Asia Pacific
Access Now

Comments to and Recommendations for the National Cybersecurity Plan 2023-2028

Submitted on July 25, 2023 by Access Now

Author of the Submission

Access Now is a human rights organization that defends and extends the digital rights of people and communities at risk. Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the continued openness of the internet and the protection of fundamental rights. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions and convenings such as RightsCon, we fight for human rights in the digital age. As an ECOSOC accredited organization, Access Now routinely engages with the United Nations in support of our mission to extend and defend human rights in the digital age, including active participation in UN cyber processes such as the Open-Ended Working Group (OEWG) and the Ad Hoc Committee deliberating a proposed international cybercrime treaty.

Access Now runs a 24/7 Digital Security Helpline, which includes incident response, threat analysis, and education and community building. It is part of the US Cybersecurity and Infrastructure Security Agency (CISA) Joint Cyber Defence Collaborative project and is the first civil society organization to become a member of the Forum for Incident Response (FIRST). Access Now is also a co-founder of the Civil Society Computer Emergency Response Team (CIVICERT) network.

Contact Persons:
Raman Jit Singh Chima
Senior International Counsel and Asia Pacific Policy Director
Global Cybersecurity Lead
raman@accessnow.org

Atty. Golda Benjamin
Campaigner for Asia-Pacific
golda@accessnow.org
+63 917 811 7007

Guide to reading proposed amendments

In this submission:

- the original text from the rules will be in *italicized fonts.*
- proposed deleted sections will be in ***BOLD, ITALICIZED LETTERS*** WITH A ***~~STRIKETHROUGH MARKER.~~***
- new sections in ***BOLD, ITALICIZED LETTERS.***

Comments to and Recommendations for the National Cybersecurity Plan 2023-2028

General comments

1. The Philippine National Cybersecurity Plan 2023-2028 should seize the opportunity to recognize human rights and fundamental freedoms in policies and strategies to secure the nation and its people. To do this, some sections could clearly articulate this vision.

   In the **Declaration of core principles (page 1)**, the following sections could read:

   > 2. *Government-enacted policies and technological controls must be centered in building anchors of trust* ***and a human-centric approach to cybersecurity****, where* ***people's human rights and fundamental freedoms are protected alongside the goals of national security and economic development.***
   >
   > *xxx*
   >
   > 7. *Internationally accepted norms in ethical behavior in cyberspace* ***and the rule of law***[1] *are adhered to, and the government aspires to be a responsible member of the international community working for cybersecurity under a rules-based framework respecting international human rights law.*

[1] Rule of Law was one of the core principles in the Philippine National Cybersecurity Plan 2022.

2. Given the vulnerability of the Philippines towards natural calamities and climate-related threats, the NCSP 2023-2028 should also emphasize on creating resilience for infrastructures, systems, and processes related to the cybersecurity of the country. This should include clear plans from the national to the local level, on disaster risk reduction, management, and recovery, which can be discussed under Pillar 2 of the draft strategy.

Pillar 1: Enact the "Cybersecurity Act" to strengthen the policy framework

3. To encourage the Philippine Congress to act with urgency and prioritize the Cybersecurity Act, the opening paragraph in Pillar 1 could read:

> **<u>Page 5.</u>** The first pillar in our strategy is to create the proper policy framework ***through the enactment of the Cybersecurity Act. A human-centric cybersecurity law, anchored in international human rights law, is urgently needed, especially because PDP 2023-2028 aims to improve e-commerce and digital trade by strengthening regulatory frameworks in areas of transparency, privacy, and cybersecurity. The proposed law reflects*** the NCSP 2023-2028 core principles outlined in Chapter 2. ***A supporting law is critical to further strengthen our second national cybersecurity plan. This section first discusses the economics of cybersecurity, the vulnerabilities of the Philippines in terms of cyberattacks, and the challenges of misaligned incentives, asymmetric information, and externalities that the proposed Cybersecurity Act seeks to address in order to create an ecosystem of mutual trust and shared responsibility when defending cyberspace.***
>
> *Delete: To better understand how we formulated these policies, let us first frame the problem that is cybersecurity and understand the economic relationships that we need to solve in order to create an ecosystem of mutual trust and shared responsibility when defending cyberspace.*

4. The proposed Cybersecurity Act is an opportunity to reflect the country's needs and align our approach with international best practices. Access Now proposes the following in relation to this proposed law:

A. **Privacy and cybersecurity crucially related to each other**: We welcome the recognition in the draft strategy document that privacy is not only a desired property of cybersecurity, but in fact constitutes an integral component of every cybersecurity strategy [Pages 3 and 4]. Privacy and cybersecurity are crucially related, and approaches that recognize strong protections and remedies on safeguarding privacy and protecting personal data are crucial to advancing effective cybersecurity.

B. **We welcome measures on cybersecurity incident reporting and wish to offer propose some points for improvement.** We comment the focus in the draft cybersecurity strategy document on outlining timely reporting requirements for cybersecurity incidents. We advise however that current language on requiring disclosures to be kept confidential could be subject to further refinement [**Page 13**]. It currently appears to desire to ensure that the NCERT will generally keep disclosures confidential ("*NCERT shall keep the disclosure confidential until such time when authority for disclosure is granted*."). It would be appropriate for the language to explicitly clarify that this would not preclude service providers from notifying impacted users of cybersecurity incidents not only to inform them, but to also ensure that they can take urgent mitigative steps as needed. The requirement that the NCIAC and NSC Director General must explicitly authorize the public disclosure of cybersecurity incidents should be altered, if not omitted. At maximum, this should be reworded as follows:

> *"2. NCERT **may** keep the disclosure confidential until such time when authority for disclosure is granted.*
> *3. The National Cybersecurity Inter-Agency Council (NCIAC) chaired by the Executive Secretary and co-chaired the by DICT and the National Security Council (NSC) Director-General [23], in its regular meeting, shall be required to authorize any decision by the NCERT restricting the public disclosure of a cybersecurity incident. Any such order shall not prevent the disclosure of a mitigated incident.*

C. We also recommend that any cybersecurity incident reporting process be harmonized with the legal text for reporting data breach

incidents to the National Privacy Commission. Therefore, the DICT should consider altering the cybersecurity incident reporting incident timeline to a maximum of within 72 hours of an incident, matching the time period set for data breach reporting. Additionally, there should be consideration of a synergized process by which the NCERT and NPC can receive joint incident reporting for cybersecurity and data breach incidents - a single window notification process, with requisite legal mechanisms permitting the same.

D. We appreciate the focus laid in the strategy on recognizing the value of the work done by security researchers and encouraging the ecosystem for them to responsibly disclose cybersecurity incidents [**Pages 13, 14, 17**]. Future laws should not allow for their unlawful surveillance, improper persecution, or harassment. The same protection should also extend to those who speak up with concerns about information security; specifically, laws must not persecute, discredit, or defame individuals who express concerns about computer systems, security mechanisms, databases, and other related tools.[2]

Advancing effective cybersecurity requires a human-centric approach that encourages and incentivizes the human beings working in cybersecurity. In that regard, we strongly support the emphasis laid in the draft strategy that security researchers should not be made subject to legal threats. We recommend however that this should not be made subject to a blanket condition that the vulnerability not be disclosed publicly; and instead focus on it being disclosed subject to appropriate responsible disclosure policies. Therefore, this would read as:

> *"Any security researcher who responsibly disclosed a vulnerability found in any asset in cyberspace, be it from a private enterprise or government agency, cannot be sued or subject to prosecution."*

[2] *See* Access Now's statement to the first session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes, March 11, 2022. Delivered by Raman Jit Singh Chima, Senior International Counsel and Global Cybersecurity Lead. Available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Statements/Access_Now_4_OP8.pdf

5. To establish a clear legislative agenda on cybersecurity, the NCSP 2023-2028 should also identify other laws needed to execute its executives: whether these are new laws or amendments to existing ones.

Pillar 2: Secure and protect Critical Information Infrastructures (CII)

6. The NCSP 2023-2028 should also consider companies from other sectors to be considered as CII, given their size in the Philippine economy. The list in **page 22** could read:

    - *Food and agriculture;*
    - *Energy, including large suppliers of energy raw materials;*
    - *Transportation;*
    - *Health including large insurance providers* ***and health information data management system providers;***
    - *Supply Chain and logistics including international sea and air ports;*
    - *Banking and finance,* ***including mobile payment systems, remittance centers, and major credit cooperatives.***
    - *Telecommunications and ISPs including operators/contractors of subsea cables and landing stations;* ~~***and***~~
    - *Manufacturing of critical goods including equipment used in defense or information security;* ***and***
    - ***All other sectors that are classified by Philippine law as public utilities.***

7. We do not support a confidentiality requirement on which organizations are designated as CII [**Page 21**]. The designation of particular entities or whole sectors as CII does not merit secrecy; such information must be ordinarily available publicly and known, so all stakeholders can be aware of the standards to be adopted in engaging such entities and have better understanding of the landscape for cybersecurity protection in the country.

Pillar 3: Proactively defend government and our people in cyberspace

8. If the Republic of the Philippines choses to more specifically designate cyberspace as a domain related to national defense, it must also indicate in its strategy its commitment to a rules-based international order that recognizes the applicability of the UN charter and international law - including international humanitarian law and international human rights law - to cyber operations. There should also be discussion on also specifically indicating a commitment

to avoiding the militarization of cyberspace, in line with later discussions in this strategy around the peaceful resolution of disputes amongst states. More specifically, the strategy should also specifically refer to the international law acquis on the applicability of international law to cyberspace as recognized in the successive reports on cyber norms of the United Nations Group of Governmental Experts (GGE) on responsible state behavior with regards to ICT, as accepted by ASEAN in its 2018 joint leaders' statement and further committed to in detail by the 2019 ASEAN cyber ministerial meeting.

9. On **page 26**, consider adding offices and departments that collect massive amount of data to deliver on its mandate and/or those that have functions relevant to cybersecurity:

    - Technology: National Privacy Commission, COMELEC
    - Economic and social prosperity: DSWD, DOH
    - National security: Office of the President

10. The NCSP 2023-2028 should also highlight the role of local government units and offices at the local level, where users' data are often collected, stored, and processed at a massive level; and where cybersecurity knowledge and security may be at its lowest vis-a-vis possible threats.

11. On **page 30:**

    A. Data classification: Cybersecurity deals with data and with people owning the data, using the data, or being impacted by data. It would be ideal for the government to already recognize a Human Rights-Based Approach to Data (HRBAD) and be guided by existing literature from the United Nations.[3]

    Number 1, Page 30. The government should be strict in applying rules in handling each class of data, along with rules on class inheritance, transition, storage, and attribute handling when multiple data classes are stored in one storage device. ***Cognizant of the users' relationship with the data that they own, use, or affect them, the Philippine cybersecurity strategy must abide by the principles of a human rights-based approach to data (HRBAD): participation, data***

[3] United Nations Office of the High Commissioner on Human Rights, *A Human Rights-Based Approach to Data: Leaving no one behind in the 2030 Agenda for Sustainable Development* (2018). Available at: https://www.ohchr.org/sites/default/files/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf

disaggregation, self-identification, transparency, privacy, and accountability.[4]

B. Supply Chain Security: Consider strengthening the language to capture enhanced due diligence for procurement of products and services by the government to ensure that cybersecurity goals are met.

Number 2, Page 30. The DICT should work with the DBM, the Government Procurement Policy Board (GPBB), ***and relevant offices*** in defining a standard for ICT products ***and services*** to be procured by government agencies ***and in conducting enhanced due diligence to ensure that the suppliers at any stage of the supply chain, both local and international, do not pose cybersecurity challenges to the country or have a history of creating cybersecurity challenges in other countries because of economic, security, geopolitical, and other motivations.*** The NCERT has seen many cases of compromised government data assets because these were stored in non-secure, non-certified products. The standard should consider the voluntary security certification system being proposed in Pillar 1 and should prescribe the minimum level of security certification or label based on the classification of data that will be handled. Currently, the DICT sees no need to create a product certification laboratory, but the private sector may be allowed to invest in security certification laboratories and systems. Likewise, mutual recognition of certification should be actively worked on.

Pillar 4: Operational and well-coordinated network of CERT and SOC

12. The NCSP 2023-2028 can also explore cooperation initiatives by the NCERT and the AFP CERT with private sector, academe, and civil society CERTS to ensure that cybersecurity learnings and challenges are continuously shared among various stakeholders. This is critical given the fact that all over the world, academicians, journalists, and activists are also constantly being threatened with cybersecurity threats that may escalate into threats against the government and businesses, depending on the actors and circumstances surrounding the threats.

[4] *Id.*

Pillar 5: Capacitate our workforce in cybersecurity

13. In *5.1 Improve the cybersecurity culture in the country* ***(page 37)***, the plan should require all government agencies and local government units to regularly perform cyber-hygiene seminars and activities, instead of limiting this to a proposed Cyber Awareness Month. In order to create a cybersecurity culture, best practices should be integrated into the workflow and practice of all stakeholders. Cybersecurity competency must also cut across different classes of government workers: from those specializing in cybersecurity to those whose mandate may be impacted by cybersecurity opportunities and challenges.

Pillar 6: Enhance international cooperation

14. Given that this is already our 2nd National Cybersecurity Plan, the NCSP 2023-2028 can be an articulation of the country's fundamental policy positions on key issues being discussed in international platforms.

15. We are optimistic that the Philippines recognizes an emerging international consensus on the global danger posed by the proliferation of the spyware industry and the growth of illegal markets offering access to, inter alia, software vulnerabilities, spyware, sophisticated high-end offensive ICT tools and "hacker for hire" services. We believe that the opportunity now clearly exists for international leadership - bolstered by the Philippines - to leave no safe space for the spyware industry to thrive.

16. The National Cybersecurity Plan 2023-2028 is also an opportunity for the Philippines to ensure that in implementing its responsibilities or commitments arising from the ASEAN Digital Masterplan 2025 and other regional and global international policy and discussion documents, are consistent with the rule of law.

- End -