JOYNEWS-YOUTH BRIDGE FOUNDATION NATIONAL DIALOGUE ON CYBER SECURITY

RESOLUTION

Preamble

We, participants at a one-day national dialogue on cybersecurity organized by Joy News and the Youth Bridge Foundation on the theme **"Strengthening Cybersecurity Protocols, Safeguarding Citizens' Vulnerabilities,"** held on March 12, 2014, at the Ecobank Head Office, Ridge, Accra;

Aimed at complementing government efforts, including the implementation of the National Cybersecurity Act 2020 (Act 1038), particularly Section 59 on Cybersecurity Standards and Enforcement, which enjoins the Cyber Security Authority to, among other things, take necessary measures to enforce the cybersecurity standards adopted and monitor compliance by the public and private sector actors.

Noting with appreciation, the support from Ecobank Ghana Limited, Hydra Cybersecurity, Ghana Enterprises Agency and Cyber Security Authority;

Acknowledged the government's efforts and the significant strides Ghana has made in advancing cyber protection measures, including the ratification of the African Union Convention on Cyber Security and Personal Data Protection, the establishment of the Cyber Security Authority, the enactment of the Data Protection Act of 2012, and public awareness campaigns on cybersecurity matters;

Emphasized the need to adopt a participatory approach in policy decision-making and implementation, hence the cyber security national dialogue to discuss critical issues of policy implementation and challenges in the cybersecurity space, including existing data protection protocols in the country;

Having deliberated on issues and challenges within the cybersecurity ecosystem, including the need to create an enabling policy and legislative environment on cybersecurity, participants…

Expressed Concern about the absence of a legislative instrument to elaborate and provide more detailed rules and regulations to provide operational guidelines and procedures set out in the Cybersecurity Act, 2020 (Act 1038\);

Recognizing that weak cybersecurity guidelines, coupled with the absence and lack of effective monitoring of institutional cyber-security protocols, have far-reaching consequences for the broader economy, particularly in the context of educational and health institutions;

Admit that cyber security issues and the need to protect citizens from vulnerabilities are collective responsibilities requiring a multistakeholder approach to strengthening the cybersecurity protocols in Ghana.

Key Learnings

- No system is unbridgeable; therefore, entities and organizations must continue to update and upgrade their systems.
- Awareness creation is crucial to safeguarding institutions and the public from cyber security threats.
- Funding for research and development is crucial to safeguarding the cybersecurity ecosystem in the country.

- Complement information infrastructure protection with regular awareness creation and education of the public on cybersecurity issues and measures put in place to protect the public.
- Cross-sector collaboration is crucial to tackling cybersecurity threats.
- Creating an enabling policy, protocol, and legislative environment for cybersecurity
- Investment in up-to-date technology and security tools is vital for the protection of critical infrastructure and public data.
- The Cyber Security Authority has set up a platform on short code 292 for the public to report cyberspace incidents and cybercrimes and receive support.

Resolve that:

CYBER SECURITY AUTHORITY (CSA)

1. **The Cyber Security Authority must intensify cybersecurity awareness and education campaigns by both public and private entities.** This should include deepening citizens education about cybersecurity threats and vulnerabilities and their responsibilities in safeguarding. This means finding better ways to educate and sensitize both the formal and informal sectors. For instance, enlightening informal and small businesses on cybersecurity threats, particularly crimes, and measures put in place by the state to protect them.

2. **Expedite action on the development and passage of the Legislative Instrument (LI):** The CSA and civil society actors should facilitate the promulgation of the needed LI to give the needed operational backing for the implementation of the CSA Act 2020 (1038).

3. **Promote multi-stakeholder collaboration and partnerships on cybersecurity issues.** *CSOs and media should in partnership with CSA jointly create a platform for sustained dialogue on cybersecurity issues*. Accordingly, the CSA should consider the input of all stakeholders, particularly end users, in the emergency response plan and ensure that emergency response information is simple, readily accessible to all, and updated.

LOCAL AND INTERNATIONAL PARTNERS

4. **Sustain the development of homegrown cyber security measures:** We need to recognize the invaluable role of local institutions in developing independent and home-grown solutions to safeguard the public against cybersecurity threats. For instance, the National Identification Authority (NIA) built a resilience system using homegrown solutions.

5. **Pursue a national sector-wide cybersecurity framework for institutions:** This should include establishing and deploying cybersecurity controls in various institutions. For example, outlining clear roadmaps and certification of the systems and practices of educational and health institutions.

6. **Funding for Research and Development:** State and non-state bodies should invest in domestic cybersecurity research to develop homegrown solutions.