



STATEMENT ON NATIONAL EFFORTS AND COMMENTS ON THE MAIN TOPICS OF THE
FIFTH MEETING OF THE OPEN-ENDED INTERGOVERNMENTAL EXPERT GROUP ON
CYBERCRIME HOLDING IN VIENNA, AUSTRIA FROM 27 – 29 MARCH 2019

*Chair,
Excellencies,
Distinguished Delegates,
Ladies and Gentlemen,*

It is a pleasure to be participating in this 05th IEG-C meeting and we thank the UNODC for staging this very important platform to exchange ideas, good practices and recommendations in the drive to strengthen the fight against Cybercrime.

2. Agenda Item 2 – Law Enforcement and Investigations

Under this agenda item, we restate the commitment of the Nigerian government and its LEAs to the progressive implementation of the National Cybersecurity Policy and Strategy and provisions of the Cybercrime (Prohibition, Prevention, Etc.) Act, 2015. The Police Special Cybercrime Unit was established to focus on investigations, in addition to the work being done by EFCC. The National Digital Forensics Laboratory also supports and enhances investigations.

In this regard, LEAs' cooperation with all stakeholders, towards creating synergy for awareness education, prevention, detection, investigation and prosecution of cybercrimes to reduce its impact on the Nigerian economy has commenced. One of such successful initiatives is the Nigerian Electronic Fraud Forum (NEFF) <https://www.cbn.gov.ng/neff/about.asp> which enhanced the cybercrime readiness of payment industry members and LEA response to the point where even though attempts have increased as predicted, payment fraud losses are on a continuous decline. This is premised on policy and institutional support for the creation of trusted information sharing platforms/sectoral CERTs/SOCs across all sectors, noting the potential to improve and transform the initiatives into a trusted and mutually beneficial mechanism, for combating cybercrime.

Capacity building is a key component for strengthening our national response to the menace of cybercrime, and Nigeria has continued to deliver relevant training and cyber capacity building programs domestically and in collaboration with development partners for LEAs. Cybercrime first responders' training and electronic evidence/forensics courses have been conducted in joint sessions to further enhance inter-agency collaboration. The GLACY+ Project of the Council of Europe and other partners have continued to provide support in this area, which has enabled several of our LEAs to participate in international trainings, collaborative meetings and relevant conferences, and must be applauded.

International cooperation – formal and informal - remains an indispensable tool for law enforcement to effectively investigate cybercrime and secure requisite evidence for effective prosecutions, and Nigeria's Central Authority Unit working tirelessly with the Cybercrime Prosecution Unit and all LEAs, continues to improve and deepen coordination and international cooperation in the fight against cybercrime. The need for capacity building in this area also cannot be overemphasized.

3. Agenda Item 3. – Electronic evidence and criminal justice

Under this agenda item, the Nigerian government recognized the fast-growing importance of electronic evidence with the attendant impact on criminal justice administration particularly, and in 2011 amended the Evidence Act to provide the requisite legal framework for admissibility of electronic evidence. Building the capacity of law enforcement and criminal justice authorities to identify existing frameworks for gathering and using electronic evidence, methods of validating and reviewing admissibility issues for electronic evidence in the investigation and trial process, etc becomes very crucial.

Cyber capacity building and international cooperation – formal and informal – are recognized as major enablers for effective investigation and prosecution of cybercrime across jurisdictions. Nigeria is committing resources to train and equip law enforcement to carry out forensically sound investigations, while respecting fundamental human rights, as well as re-organization of the educational curriculum to help address the growing skilled manpower challenges.

Relatively, the interaction/impact of data protection laws have a direct effect on requests for electronic evidence in cross-border crimes and international judicial cooperation, thus making the development of the Data Protection legislation in Nigeria increasingly more important. In this regard, the development of the Data Protection Bill, 2019 has been completed with the support of the GLACY+ Project and the World Bank and is now at the final stages of the legislative process, after which it will be sent for Presidential assent.

To further strengthen both the legal framework and cooperation relating to electronic evidence, it is noteworthy that Nigeria has been invited to accede to the Convention on Cybercrime (ETS No.185) and consultations are now ongoing for the final approval for Nigeria's accession to the Budapest Convention. Nigeria, as an observer nation, is also actively following the negotiations/ preparation of a draft 2nd Additional Protocol to the Budapest Convention on Cybercrime.

The Cybercrime Advisory Council has also finalized plans to roll out a cybersecurity awareness campaign in 2019 to drive citizen enlightenment and general cyber hygiene.

4. To conclude, Chairperson, Nigeria reiterates that technology holds the key for a brighter future. It provides access to education, promotes freedom of speech, connects people across the globe and enables delivery of essential services. There is an increasing evidence of strong link between internet connectivity and social and economic empowerment. The internet empowers people from all walks of life. Cybercrime in that regard, threatens our fundamental human rights and is one of the most prevalent and organized crimes on the rise today. As a result of the threat cybercrime poses to humanity, it is essential to empower law enforcement to conduct investigations, access and retrieve electronic evidence in a forensically sound manner, to better manage the complex fight against the increasing danger of cybercrime; and to learn from one another, most especially the practical aspects of combatting cybercrime including experiences implemented nationally by Member States as well as public-private partnerships.

Thank you all for your kind attention.

T. George-Maria TYENDEZWA, CFE
Assistant Director |Head,
Cybercrime Prosecution Unit,
Federal Ministry of Justice, Abuja, Nigeria
E: terlumun.tyendezwa@justice.gov.ng
Alt: TyendezwaTG@cybersecurity.gov.ng
W: www.justice.gov.ng