MINISTRY OF COMMUNICATIONS AND DIGITALISATION GHANA

CYBER SECURITY AUTHORITY CSA

NATIONAL CYBER SECURITY AWARENESS MONTH 2021

GHANA'S CYBERSECURITY ACT 2020

ITS IMPLICATIONS AND THE ROLE OF STAKEHOLDERS

OCTOBER 1ST-31ST 2021

LIVE STREAMING YouTube LIVE

www.cybersecurity.gov.gh


SOS

TABLE OF CONTENT

National Cybersecurity Leadership

H. E. NANA ADDO DANKWA AKUFO-ADDO
President of the Republic of Ghana

H. E. ALHAJI DR. MAHAMUDU BAWUMIA
Vice President of the Republic of Ghana

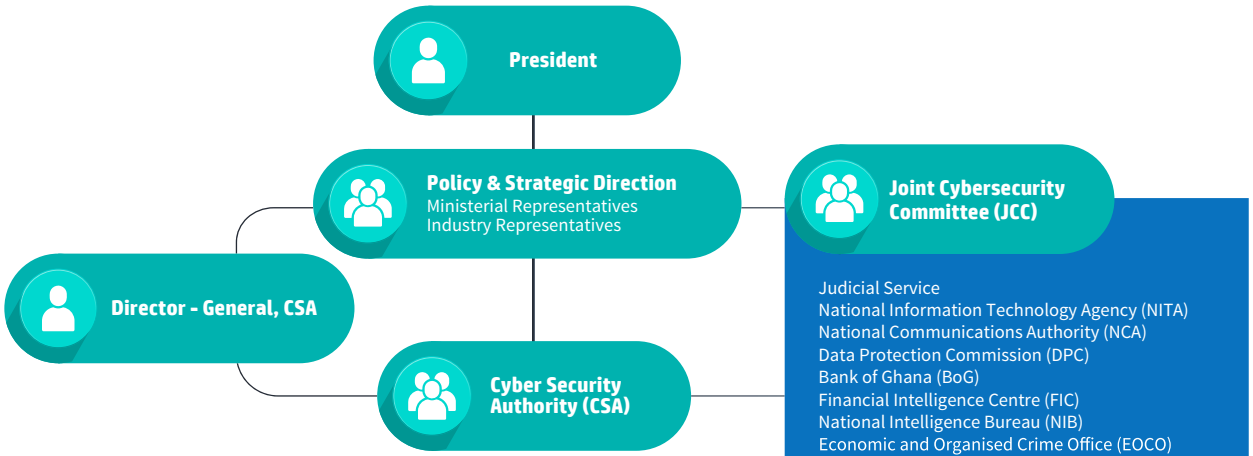
MRS. HON. URSULA OWUSU-EKUFUL (MP)
Minister for Communications & Digitalisation

HON. AMA POMAA BOATENG
Dep. Minister for Communications & Digitalisation

MRS. MAGDALENE APENTENG
Chief Director, Ministry of Communications & Digitalisation

DR. ALBERT ANTWI-BOASIAKO
Ag. Director-General, Cyber Security Authority (CSA)

National Cybersecurity Governance Structure



Non-Governmental Representatives

- → Private Sector
- → Business
- → Civil Society Organisations
- → Academia
- → International Partners / Organisations
- → Professional / Industry Associations

Overview of the Cybersecurity Act, 2020 (Act 1038)

Ghana's new legislation on Cybersecurity is considered a landmark intervention to propel the country's cybersecurity development. The President H.E. Nana Addo Dankwa Akufo-Addo assented the Cybersecurity Act, 2020 (Act 1038) into law on December 29, 2020, after it was passed by Parliament on November 06, 2020.

Act 1038 establishes the Cyber Security Authority (CSA), provides a comprehensive legal framework for the protection of the critical information infrastructure of the country, regulates cybersecurity activities including licensing of cybersecurity services, provides for the protection of children on the internet and develops Ghana's cybersecurity ecosystem. It is also targeted at positioning Ghana to prevent, manage and respond to cybersecurity incidents in view of our digital transformation agenda.

The memorandum accompanying the introduction of the law signed by the Hon Mrs. Ursula Owusu-Ekuful, indicated that, a successful economy is hinged on a secured, safe and resilient national digital ecosystem. Cybersecurity is, therefore, very critical to the economic development of the country and essential to the protection of the rights of individuals within the national digital ecosystem'.

The implementation of the Act is expected to re-affirm Ghana's leadership on cybersecurity matters in the sub-region.

With the passage of Act 1038, the National Cyber Security Centre (NCSC) will transition into the Cyber Security Authority (CSA).

Overview of the Cyber Security Authority (CSA)

The Cyber Security Authority (CSA) has been established by the Cybersecurity Act, 2020 (Act 1038) to regulate cybersecurity activities in the country; to promote the development of cybersecurity in the country and to provide for related matters.

The CSA officially started operations on 1st October 2021; starting as the National Cyber Security Secretariat (NCSS) with the appointment of the National Cybersecurity Advisor in 2017 and later transitioned into the National Cyber Security Centre (NCSC) in 2018 as an agency under the then Ministry of Communications and Digitalisation.

1. Mandate and Functions of the CSA

01 Regulate cybersecurity activities in the country.

02 Prevent, manage and respond to cybersecurity threats and cybersecurity incidents.

03 Regulate owners of Critical Information Infrastructure in respect of cybersecurity activities, cybersecurity service providers and practitioners in the country.

04 Promote the development of cybersecurity in the country to ensure a secured and resilient digital ecosystem.

05 Establish a platform for cross-sector engagements on matters of cybersecurity for effective co-ordination and co-operation between key public institutions and the private sector.

06 Create awareness of cybersecurity matters.

07 Collaborate with international agencies to promote the cybersecurity of the country.

Vision

To ensure a ***Secure and Resilient Digital Ghana.***

Mission of the CSA

To ***Build a Resilient Digital Ecosystem; Secure Digital Infrastructure; Develop National Capacity; Deter Cybercrime;*** and ***Strengthen Cybersecurity Cooperation.***

Core Values

Confidentiality

Inclusiveness

Integrity

Commitment

Reliability

Professionalism

Key Milestones/Engagements

01 Establishment of **National Cybersecurity Institutional Framework**

02 Enactment of the **Cybersecurity Act, 2020 (Act 1038)**

03 Revision of the **National Cybersecurity Policy and Strategy**

04 Establishment of **Cyber Security Authority (CSA)**

05 Ratification of the **Convention on Cybercrime** (Budapest Convention) in 2018

06 Ratification of the **African Union Convention on Cyber Security and Personal Data Protection** (Malabo Convention) in 2019

Key Milestones/Engagements

07 Development of a **Directive for the Protection of Critical Information Infrastructure (CII)**

08 Establishment of National and Sectoral Computer Emergency Response Teams (CERTs)

09 Establishment of **Cybercrime/ Cybersecurity Incident Reporting Points of Contact (POC)**

10 Jointly signed the **Digital Inclusion Statement** with the Government of Germany

11 Capacity building for the Criminal Justice Sector in cybercrime and electronic evidence handling (GLACY+ Project)

12 Development and adoption of the ECOWAS' **Regional Cybersecurity Cybercrime Strategy & Regional Critical Infrastructure Protection Policy** in 2021

Key Milestones/Engagements

13 Membership of **Forum of Incident Response Security Teams (FIRST)**

14 Membership of **Global Forum on Cyber Expertise (GFCE)**

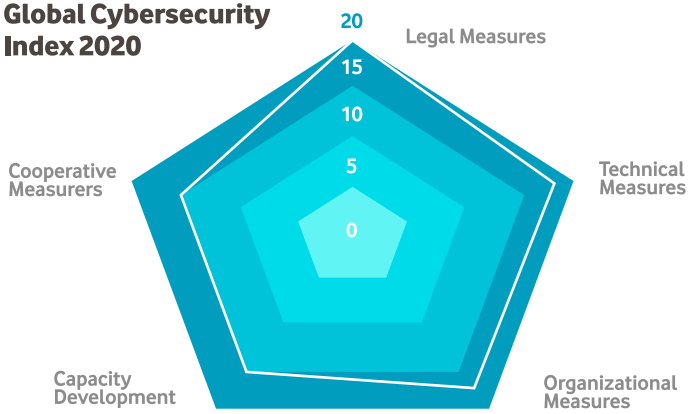
15 International Partnerships

- Freedom Online Coalition (FOC)
- World Bank
- Security Governance Initiative (SGI)
- UNICEF
- International Telecommunication Union (ITU)
- World Economic Forum (WEF)
- ECOWAS
- United Nations (UN)
- African Union (AU)
- Global Internet Forum to Counter Terrorism (GIFCT)
- European Union
- UK Home Office (NCRA Project)
- Council of Europe (GLACY+ Project)

Highlight of Ghana's ITU Global Cybersecurity Index Rating

Year	Score	Africa Ranking	Global Ranking
2017	32.6%	10th	87th
2020	^ 86.69%	3rd	43rd

Global Cybersecurity Index 2020



Development Level
Developing Country

Area(s) of Relative Strength
Legal, Technical Measures

Area(s) of Potential Growth
Capacity Development, Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measurers
86.69	19.35	18.48	17.78	15.44	15.63

Directive for the Protection of Critical Information Infrastructure (CII)

Critical Information Infrastructure (CII) constitutes assets (real/virtual), networks, systems, processes, information, and functions that are vital to the nation such that their incapacity or destruction would have a devastating impact on national security, the economy, public health and/or safety. CII may comprise a number of different infrastructures with essential interdependencies and critical information flows between them. The Cybersecurity Act, 2020 (Act 1038) defines a critical information infrastructure as a computer system or computer network that is essential for national security or the economic and social well-being of citizens.

Cyber-attacks against CIIs are increasing, the magnitude, frequency and impact of such security incidents can impede the pursuit of economic activities, generate substantial disruption to critical services, financial losses, undermine public confidence, and cause major disruption to our economy. Recent attacks on the power grids, electoral systems, payment systems and healthcare systems around the world bring to bear the imminent threats to Ghana's CII. It's only a matter of time before we also fall victim, and we must be prepared for this eventuality.

In the last few years, Ghana has implemented a number of digitalisation initiatives as we modernise networks and information systems to meet relevant developmental agenda, both in the public and the private sectors, and to facilitate the growth of the economy. Some of these networks and information systems form a substantial part of Ghana's CII. They underpin many of the critical services used in daily life, from functions as diverse as financial payments to air traffic control.

The protection of CII is the shared responsibility of both public and private organisations that own and operate CIIs. To ensure a safer and resilient digital ecosystem, there is a need to adopt a framework to ensure the confidentiality, integrity, and availability of Ghana's CII and to minimise the likelihood and impact of successful cyber-attacks against our CII. Ghana must secure its infrastructure, deter cybercrime, develop

national capacity, build a resilient digital ecosystem relative to cybersecurity, and strengthen cybersecurity cooperation among critical sectors. The protection of CII constitutes the backbone of Ghana's digital resiliency.

The **Directive for the Protection of Critical Information Infrastructure (CII)** to CII Owners, is issued to CII Owners to protect CII pursuant to Section 92 of Act 1038. The Directive establishes baseline cybersecurity requirements for all designated CII Owners; procedures for incident response as well as requirements and procedures for audit and compliance enforcements by the Authority; and outlines the technical and organisational measures to be adopted by designated CII owners in protecting the CII systems and networks.


Designated CII Sectors
National Security & Intelligence
Information & Communication Technology (ICT)
Banking and Finance
Energy
Water
Transport
Health
Emergency Services
Government
Food and Agriculture
Manufacturing
Mining
Education
NATIONAL AMBULANCE SERVICE

NCSAM 2021 Concept Note

1. Background

The 7th Parliament of the Republic of Ghana, on November 06, 2020, passed the historic Cybersecurity Act, 2020 (Act 1038), which was subsequently assented into law by the President H.E. Nana Addo Dankwa Akufo-Addo on December 29, 2020. The Act addresses the gaps in the existing domestic legislation with respect to Ghana's cybersecurity development. The Act provides a legal basis for the establishment of the Cyber Security Authority (CSA) to regulate cybersecurity activities; to protect critical information infrastructure; to provide for the development of the Computer Emergency Response Team (CERT); to promote public awareness and education on cybersecurity matters, and to provide for related matters.

As part of measures to effectively implement Act 1038, the National Cyber Security Centre (NCSC) of the Ministry of Communications and Digitalisation (MoCD) seeks to leverage on the 2021 edition of the annual National Cyber Security Awareness Month (NCSAM) to raise awareness and build capacity on this important development through the theme ***"Ghana's Cybersecurity Act 2020; Its Implications and the Role of Stakeholders."*** Therefore NCSAM 2021 seeks to engage with relevant stakeholders to deliberate on the Act and its implications, as Ghana seeks to build upon its foundational cybersecurity pillars, which has been ranked 3rd on the African continent with a rating of 86.69% according to the ITU's Global Cybersecurity Index report, 2020.

2. Objectives of the National Cyber Security Awareness Month (NCSAM) 2021

The month-long event aims to:

- Officially launch the ***Cyber Security Authority (CSA)*** with a mandate to commence its full regulatory mandate.
- Launch the ***Critical Information Infrastructure (CII) Directive*** which is designed to protect designated CIIs from cyber-attacks.
- Create awareness on the ***Cybersecurity Act, 2020*** and cybercrime trends while building capacity on cybersecurity among Ghanaians.

- Build upon the ***Safer Digital Ghana*** campaign by creating awareness among Children, the Public, Businneses and the Government.

- Create a platform to improve local and international cooperation and partnerships to fight cybercrime and improve cybersecurity, consistent with Act 1038.

3. Expected Outcome

The month-long event is expected to:

- Establish the Cyber Security Authority (CSA) to commence the implementation of the provisions of Act 1038 to protect Ghana's developing digital ecosystem.

- Establish and implement protection mechanisms for all designated Critical Information Infrastructure (CII) based on the guidelines outlined in the CII Directive.

- Improve awareness on the Cybersecurity Act among key stakeholders and the Ghanaian public at large.

- Increase awareness of the cybercrime/cybersecurity incidents reporting Points of Contact (PoC) to facilitate reporting of cybercrime and cybersecurity incidents.

- Strengthen formal and informal cooperation at local and international levels on cybercrime/cybersecurity-related matters to effectively implement Act 1038.

4. Focus Areas

The NCSAM 2021 will focus on key areas of Ghana's cybersecurity development based on Act 1038, including the following;

- Critical Information Infrastructure (CII) protection
- Computer Emergency Response Teams (CERTs)
- Capacity Building and Awareness Creation (CBAC)
- Child Online Protection (COP)
- Media related activities/engagements to raise awareness on the newly established Cyber Security Authority and its mandate.

5. Major Highlights

i. Official Launch of National Cyber Security Awareness Month (NCSAM) 2021, a Directive for the protection Critical Information Infrastructure (CII) and the Cyber Security Authority (CSA)

The Minister for Communications and Digitalisation (MoCD) will formally launch the 2021 edition of the NCSAM on Friday, October 1, 2021. Key stakeholders from government and non-government institutions including CII owners, the media fraternity, and Ghana's cybersecurity international partners will comprise participants for the event.

ii. High-level & Regional Engagements on the Cybersecurity Act, 2020 (Act 1038)

The NCSC seeks to undertake regional sensitisation activities in the 16 regions of Ghana to educate stakeholders on the Cybersecurity Act 2020, cybercrime trends and build capacity on cybersecurity matters. It will comprise direct engagements, virtual engagements, partnerships with regional associations and media engagements via selected media outlets (television and radio) across the country.

iii. High-level Events

High-level events will be conducted each week of the month. Some of the key activities scheduled as part of the programme include:

- Launch of a ***Directive for the Protection of Critical Information Infrastructure (CII)*** and the ***Cyber Security Authority (CSA)***
- Workshop on Cybersecurity Act, 2020 for Cybersecurity Service Providers & Professionals
- Civil Society Forum on the Implementation of the Cybersecurity Act, 2020
- Forum on Women in Technology and Cybersecurity

6. Methodology

Activities will be conducted in a ***hybrid format*** comprising physical engagements (under strict COVID-19 protocols) and the utilisation of available virtual platforms and media channels. It will involve thought-leadership sessions, workshops, lectures, demonstrations, training sessions, and media engagements.

7. Participation and Attendance

The month-long awareness programme is expected to witness the participation of the Minister for Communications and Digitalisation, Deputy Minister for Communications and Digitalisation, other sector Ministers/ Deputy Ministers, members of the National Cyber Security Technical Working Group (NCSTWG), representatives from government and non-government institutions, Ghana's cybersecurity international partners, the media fraternity among others.

8. Event Venue and Other Locations

The Official Launch of NCSAM 2021 will take place in the NCA Conference Room, 2nd Floor, NCA Tower, Airport City, Accra. Other events will take place at event-specific venues based on the target audience and expected numbers. Regional events will take place at designated locations in the various target regions. Media will also host a number of activities during the month.

9. Event Dates

- The NCSAM 2021 will span from October 1-31, 2021.
- The formal launch of the NCSAM 2021, the Cyber Security Authority (CSA), and the Critical Information Infrastructure (CII) Directive will be on **Friday, October 1, 2021.**
- High-level events and other media engagements will run from October 4-29, 2021.

10. Post-Event Activities

An event survey form will be developed to collate feedback and recommendations on the NCSAM 2021 activities from participating institutions and officials. There will be the development of an official NCSAM 2021 Report after the event.

NCSAM 2021 Programme of Activities

DAY 1 | FRIDAY OCTOBER 1, 2021

OFFICIAL LAUNCH OF NATIONAL CYBER SECURITY AWARENESS MONTH (NCSAM) 2021, A DIRECTIVE FOR THE PROTECTION CRITICAL INFORMATION INFRASTRUCTURE (CII) AND THE CYBER SECURITY AUTHORITY (CSA)

Time	Session	Activity	Speaker/ Lead
09.00	1.1A	Arrival of Guests	
09.30	1.2A	Interlude/National Anthem	Police Band
10.00	1.3A	Opening Prayer	Representative from Christian Council of Ghana
10.05	1.4A	Welcome Address	Mr. Joe Anokye, Director- General, National Communications Authority
10.10	1.5A	Opening Remarks	Dr. Albert Antwi-Boasiako, National Cybersecurity Advisor
10.15	1.6A	Remarks	Dr. Maxwell Opoku-Afari, 1st Deputy Governor, Bank of Ghana
10.20	1.7A	Remarks	Amb. Stephanie S. Sullivan, USA Ambassador to Ghana
10.25	1.8A	Remarks	Hon. Mathew Opoku Prempeh, Minister for Energy
10.35	1.9A	Keynote Address and Official Launch of National Cyber Security Awareness Month 2021, Launch of Cyber Security Authority and the Critical Information Infrastructure (CII) Directive	Hon. Ursula Owusu-Ekuful, Minister for Communications and Digitalisation

Time	Session	Activity	Speaker/ Lead
10.50	1.10A	Vote of Thanks	Mrs. Magdalene Apenteng, Chief Director, Ministry of Communications and Digitalisation
10.55	1.11A	Closing Prayer	Representative of the National Chief Imam of Ghana
11.00	1.12A	Photograph	
11.05	1.13A	Unveiling of the Official Logo of the Cyber Security Authority (CSA) on 3rd Floor, NCA Tower	Hon. Ursula Owusu-Ekuful, Minister for Communications and Digitalisation
11.10	1.14A	Interview (Dignitaries)	
11.10 -12.00	1.15A	Refreshment/Networking	

Major High-Level Events

S/N	Date	Programme/ Activity	Brief Description	Approach
1	(Monday) October 11, 2021	Forum on Cybersecurity Act, 2020 for Cybersecurity Service Providers & Professionals	The forum is expected to create awareness on the Cybersecurity Act, 2020 (Act 1038) among cybersecurity service providers and professionals, to outline a clear roadmap and responsibilities for collaborative engagements between the Cyber Security Authority (CSA) and the cybersecurity industry.	Hybrid (Physical & Virtual)
2	(Monday) October 18, 2021	Civil Society Forum on the Implementation of the Cybersecurity Act, 2020	The Forum is expected to engage civil society organisations and think tank groups to deliberate and explore ideas for the effective implementation of the Cybersecurity Act, 2020 (Act 1038).	Hybrid (Physical & Virtual)
3	(Monday) October 25, 2021	Forum on Women in Technology and Cybersecurity	The Forum is expected to engage with women in IT and cybersecurity disciplines for thought-provoking deliberations to devise strategies to guide the path of young women, children and people interested to make a career in the IT field. Additionally, the forum is aimed at establishing collaboration and partnership with women in leadership roles in technology and cybersecurity for the collective goal of promoting the country's cybersecurity development.	Physical

Engagements Related to the Protection of Critical Information Infrastructure (CII)

S/N	Date	Programme/ Activity	Brief Description	Approach
1	(Monday) October 4, 2021	Workshop on the Cybersecurity Act, 2020 and Critical Information Infrastructure (CII) Directive for Identified CII Owners (Morning Session)	The workshop is expected to equip designated CII Owners with adequate knowledge and understanding of the Cybersecurity Act, 2020 (Act 1038) and Directive for the Protection of CII. Targeted stakeholders involve CII Owners from the Information Communication Technology (ICT), National Security and Intelligence, and Government Sectors.	Virtual Platform
2	(Monday) October 4, 2021	Workshop on the Cybersecurity Act, 2020 and Critical Information Infrastructure (CII) Directive for Identified CII Owners (Afternoon Session)	The workshop is expected to equip designated CII Owners with adequate knowledge and understanding of the Cybersecurity Act, 2020 (Act 1038) and Directive for the Protection of CII. Targeted stakeholders involve CII Owners from the Health, Education, and Food and Agriculture Sectors.	Virtual Platform
3	(Tuesday) October 5, 2021	Workshop on the Cybersecurity Act, 2020 and Critical Information Infrastructure (CII) Directive for Identified CII Owners (Morning Session)	The workshop is expected to equip designated CII Owners with adequate knowledge and understanding of the Cybersecurity Act, 2020 (Act 1038) and Directive for the Protection of CII. Targeted stakeholders involve CII Owners from the Banking and Finance, Emergency Services and Water Sectors.	Virtual Platform

Engagements Related to the Protection of Critical Information Infrastructure (CII)

S/N	Date	Programme/ Activity	Brief Description	Approach
4	(Tuesday) October 5, 2021	Workshop on the Cybersecurity Act, 2020 and Critical Information Infrastructure (CII) Directive for Identified CII Owners (Afternoon Session)	The workshop is expected to equip designated CII Owners with adequate knowledge and understanding of the Cybersecurity Act 2020 (Act 1038) and Directive for the Protection of CII. Targeted stakeholders involve CII Owners from the Energy, Transport, Manufacturing and Mining Sectors.	Virtual Platform

Engagements Related to the Development of the Computer Emergency Response Team (CERT) Ecosystem

S/N	Date	Programme/ Activity	Brief Description	Approach
1	(Wednesday) October 13, 2021	Workshop on Managing Cybersecurity Operations in the Telecommunications Sector	The Workshop on Governing and Managing Cybersecurity in the Telecommunications Sector aims to help all teams develop understanding of the cybersecurity eco-system in the telecommunications sector, share knowledge and lessons within the sector, and put into practice communications in the telecommunications sector through an exercise or drill.	Virtual Platform
2	(Thursday) October 14, 2021	Workshop on the Impact of the New Cybersecurity Act, 2020 (Act 1038) on CERT Operations	The workshop is expected to focus on relevant Sections of Act 1038 that impact the operations of Computer Emergency Response Teams. The event will further highlight the responsibilities of Sector CERTs for the effective implementation of the Act.	Virtual Platform

Capacity Building for Public Sector Officials

S/N	Date	Programme/ Activity	Brief Description	Approach
1	(Thursday) October 21, 2021	Capacity Building on the Cybersecurity Act, 2020 for Selected Members of Parliament	The workshop is expected to build the capacity and knowledge of selected Members of Parliament on cybersecurity-related matters and the Cybersecurity Act, 2020 (Act 1038).	Hybrid (Physical & Virtual)

Engagements Related to Child Online Protection (COP)

S/N	Date	Programme/ Activity	Brief Description	Approach
1	(Tuesday) October 26, 2021	Collaborative workshop on Child Online Protection (COP) related provisions in the Cybersecurity Act, 2020 for Colleges of Education	The workshop is expected to educate and sensitise teacher trainees on the Child Online Protection provisions in the Cybersecurity Act, 2020 (Act 1038) for the stakeholders to appreciate the need for COP in the educational sector while incorporating the culture and mindset of COP in the stakeholders.	Hybrid (Physical & Virtual Platform)
2	(Wednesday) October 27, 2021	Workshop on the Implementation of the Child Online Protection Provisions in the Cybersecurity Act, 2020 for Telecommunications Service Providers	The workshop is expected to equip telecommunications service providers with the knowledge on the Child Online Protection provisions in the Cybersecurity Act, 2020 (Act 1038) and enhance awareness creation of the stakeholders in the cybersecurity and Child Online Protection ecosystem.	Hybrid (Physical & Virtual Platform)

Priority International Cooperation Engagement

S/N	Date	Programme/ Activity	Brief Description	Approach
1	(Thursday) October 14, 2021	Global Internet Forum to Counter Terrorism (GIFCT), Tech Against Terrorism and National Cyber Security Centre Multi-Stakeholder Workshop	The workshop is expected to bring together a broad geographic and multi-stakeholder participation for the sharing of best practices and knowledge.	Virtual Platform

Capacity Building Engagements for the Criminal Justice Sector

S/N	Date	Programme/ Activity	Brief Description	Approach
1	(Tuesday) October 5, 2021	Workshop on Law Enforcement Agency Training Strategies	The workshop focuses on raising awareness on the need of a strategic approach on the cybercrime and digital forensic training.	Virtual Platform
2	(Wednesday) October 6, 2021	Workshop on the Integration of European Cybercrime Training and Education Group Training Materials	The workshop focuses on providing practical advice on scoping cybercrime and digital forensics training strategy	Virtual Platform
3	(Friday) October 15, 2021	Workshop on the New Cybersecurity Act, 2020 for the Criminal Justice Sector	The workshop is expected to build the capacity of authorities within the criminal justice sector on the New Cybersecurity Act, 2020 (Act 1038), its implications on the activities of the sector and the specific role of the stakeholders in implementation.	Physical

Capacity Building Engagements for the Criminal Justice Sector

S/N	Date	Programme/ Activity	Brief Description	Approach
4	(Monday-Tuesday) October 18 – 19, 2021	Advisory Workshop on the Streaming of Procedures for MLA enhanced by the Second Additional Protocol related to Cybercrime and Electronic Evidence	The workshop seeks to examine areas that may require support through the GLACY+ project (through capacity building activities), and to highlight the potential in Ghana of streamlining procedures for mutual legal assistance related to cybercrime and electronic evidence so that criminals are not potentially allowed a window of impunity.	Hybrid (Physical & Virtual)
5	(Wednesday – Friday) October 20 -22, 2021	Specialised Course on International Cooperation for Prosecutors and Judges	The workshop is expected to equip participants with the required knowledge on the international cooperation provisions in the Cybersecurity Act, 2020 (Act 1038) to guide effective investigation and prosecution of cybercrime.	Hybrid (Physical & Virtual)
6	(Thursday) October 28, 2021	Workshop on the New Cybersecurity Act, 2020 for the Criminal Justice Sector	The workshop is expected to build the capacity of authorities within the criminal justice sector on the New Cybersecurity Act, 2020 (Act 1038), its implications on the activities of the sector and the specific role of the stakeholders in implementation.	Physical
7	(Friday) October 29, 2021	Sod-cutting ceremony for Cybercrime and Digital Forensics Laboratory	The Ceremony seeks to cut sod for the construction of an ultra-modern Cybercrime and Digital Forensics Laboratory for the Northern Sector.	Physical

High-Level & Regional Engagements on the Cybersecurity Act, 2020 (Act 1038)

OCTOBER 1-31, 2021

Activity	Description	Target Institution/Group
Regional Engagement on the New Cybersecurity Act, 2020 (Act 1038)	Workshops will be held in the sixteen (16) regions of the country to sensitive target groups on the Cybersecurity Act and its implications.	The Authority will be engaging different groups and institutions including, Regional Security Council (REGSEC), Ghana Bar Association (GBA), Ghana Chamber of Commerce, Institute of Chartered Accountants Ghana (ICAG), Ghana Journalists Association (GJA) and other interest groups across different sectors.

BANK OF GHANA'S DOMESTIC GOLD PURCHASE PROGRAMME

Bank of Ghana's Domestic Gold purchase programme, launched on 17th June 2021, has paved the way for the Bank to grow its foreign exchange reserves to foster confidence, enhance currency stability, create a more attractive environment for foreign direct investments and economic growth. It enables the Bank to leverage its gold holdings to raise a cheaper source of financing to provide short-term foreign exchange liquidity.

www.bog.gov.gh thebankofghana thebankofghana

unicef

FOR EVERY CHILD, A SAFE ONLINE ENVIRONMENT

www.unicef.org


HUAWEI


Rayzone Group

Global Action on Cybercrime Extended – GLACY+

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

HOMEBASE TELEVISION

MEDIA FOUNDATION FOR WEST AFRICA

GHone TV

Homebase Television has been operating for the past 10 years broadcasting accurate and relevant information to Ghanaians home and in the Diaspora. Our content is mostly in the Akan local dialect centers on News, Interviews, Documentaries, Current Affairs, Entertainment and Events. In this era where the use of technology is wide spread, we believe we are the medium to bridge the gap between the locals and experts as we partner with the National Cyber Security Centre to mitigate cyber fraud in the country.

103.5 fm STARR
Simply The Best

Partners & Sponsors

Thank you to all our Partners and Sponsors working collaboratively to build a robust cyber security ecosystem in Ghana

Partners

Sponsors

Partners & Sponsors

Organising Partners

Media Partners

Notes

A Secure and Resilient Digital Ghana

Cyber Security Authority
3rd Floor, NCA Tower
KIA, 6 Airport By-pass Rd., Accra
Digital Address: GL-126-7029

Tel: +233 050 3185846
E-mail: info@cybersecurity.gov.gh
www.cybersecurity.gov.gh

Cyber Security Ghana
@cybersecurityghana
@NCSC_Ghana