



MINISTRY OF  
COMMUNICATIONS &  
DIGITALISATION



NATIONAL  
CYBER SECURITY  
AWARENESS MONTH

20  
23

# PROMOTING A CULTURE OF DIGITAL SAFETY



CHILDREN



PUBLIC



BUSINESS



GOVERNMENT



# CYBER SECURITY AUTHORITY (CSA)

# TABLE OF CONTENT



<b>i</b>	Acknowledgement
<b>ii</b>	Acronyms
<b>iii</b>	Executive Summary
<b>iv</b>	National Cybersecurity Leadership
<b>v</b>	Overview of the Cybersecurity Act
<b>vii</b>	Mandate of the CSA
<b>viii</b>	Institutional Framework
<b>ix</b>	CSA Governing Board
<b>x</b>	Joint Cybersecurity Committee
<b>xi</b>	Overview of the CSA



- 01** Media Launch of the National Cyber Security Awareness Month (NCSAM) 2023
- 06** Official Launch of the 2023 Edition of the National Cyber Security Awareness Month (Promoting a Culture of Digital Safety)
- 11** Joint Cybersecurity Committee (JCC) / Joint Intelligence Committee (JIC) Related Events
- 32** High Level Capacity Building and Awareness Creation Events
- 48** The National Cybersecurity Challenge (NCC)
- 53** Cybersecurity Collaborative Workshops
- 62** NCSAM 2023 Media Engagements
- 68** Photo Gallery



# Acknowledgement



## **Dr. Albert Antwi-Boasiako**

Director-General  
Cyber Security Authority (CSA)

As the Director-General of the Cyber Security Authority, I reflect on the success of the 2023 edition of the National Cyber Security Awareness Month (NCSAM) with a deep sense of pride and gratitude. The theme for this year's celebration was "Promoting a Culture of Digital Safety". Involvement of key industry stakeholders and the general public throughout this event reinforces our collective commitment towards a secure cyberspace.

I extend my appreciation to the Honourable Minister for Communications and Digitalisation, Mrs. Ursula Owusu-Ekufu for her exemplary leadership, vision and guidance which have propelled our efforts to new heights, fostering a more secure and resilient digital landscape for our citizens. The Minister for National Security, Hon. Kan Dapaah is acknowledged and appreciated for his support, especially during the launch of the NCSAM. My heartfelt gratitude to the Deputy Minister for Communications and Digitalisation, Hon. Ama Poma Boateng, for her commitment to promoting a culture of digital safety and for her support during the NCSAM Media Launch and the Official Launch. I am grateful to Mr. Mactar Yedaly, the GC3B Special Envoy for delivering the keynote address and to the Deputy Country Representative of UNICEF Ghana, Mr. Fiachra McAsey for his insightful remarks at the official launch.

I would like to extend my sincere appreciation to the Joint Cybersecurity Committee (JCC) and the Joint Intelligence Committee (JIC) for their invaluable contributions and unwavering commitment to the success of the Annual Cyber Security Awareness Month celebration.

Special appreciation goes to Heads and Chief Directors of Ministries and agencies who graced the event and offered diverse support. The steadfast support of the members of the CSA Governing Board and the dedication of the Management and Staff of the Authority have been the driving force behind the seamless execution of diverse activities throughout the celebration and I am grateful to them. Much would not have been achieved without the support of industry partners and collaborators, sponsors and partners; thank you all for making this awareness campaign a resounding success.

# Acronyms

<b>AI</b>	Artificial Intelligence	<b>GNFS</b>	Ghana National Fire Service
<b>AT Ghana</b>	AirtelTigo Ghana	<b>GoAML</b>	Go Anti-Money-Laundering System
<b>AU</b>	African Union	<b>GPS</b>	Ghana Prisons Service
<b>BBC</b>	British Broadcasting Cooperation	<b>GRA</b>	Ghana Revenue Authority
<b>BEC</b>	Business Email Compromise	<b>GSA</b>	Ghana Shippers Authority
<b>BNI</b>	Bureau for National Investigations	<b>HTTPs</b>	Hypertext Transfer Protocol Secure
<b>BoG</b>	Bank of Ghana	<b>IBM</b>	International Business Machine
<b>CBAC</b>	Capacity Building and Awareness Creation	<b>ICT</b>	Information and Communications Technology
<b>CEO</b>	Chief Executive Officer	<b>IDEA</b>	Institute for Democracy and Electoral Assistance
<b>CFO</b>	Chief Fire Officer	<b>IIPGH</b>	Institute of ICT Professionals Ghana
<b>CERT-GH</b>	Computer Emergency Response Team Ghana	<b>IT</b>	Information Technology
<b>CEs</b>	Cybersecurity Establishments	<b>ISACA</b>	Information Systems Audit and Control Association
<b>CIA</b>	Confidentiality, Integrity and Availability	<b>ITU</b>	International Telecommunication Union
<b>CID</b>	Criminal Investigations Department	<b>JCC</b>	Joint Cybersecurity Committee
<b>CII</b>	Critical Information Infrastructure	<b>JIC</b>	Joint Intelligence Committee
<b>CIRP</b>	Computer Incident Response Plan	<b>JTI</b>	Judicial Training Institute
<b>CISO</b>	Chief Information Security Officer	<b>KAIPTC</b>	Kofi Annan International Peacekeeping and Training Centre
<b>CMM</b>	Capacity Maturity Model	<b>KNUST</b>	Kwame Nkrumah University of Science and Technology
<b>CoE</b>	Council of Europe	<b>LECO</b>	Legal and Compliance
<b>COP</b>	Child Online Protection	<b>LELU</b>	Law Enforcement Liaison Unit
<b>CPs</b>	Cybersecurity Professionals	<b>LI</b>	Legislative Instruments
<b>CSA</b>	Cyber Security Authority	<b>MFA</b>	Multi-Factor Authentication
<b>CSOs</b>	Civil Society Organisations	<b>MoCD</b>	Ministry of Communications and Digitalisation
<b>CSPs</b>	Cybersecurity Service Providers	<b>Mol</b>	Ministry of Information
<b>DDoS</b>	Distributed Denial of Service	<b>MoMo</b>	Mobile Money
<b>DPC</b>	Data Protection Commission	<b>NACOC</b>	Narcotics Control Commission
<b>EC</b>	Electoral Commission	<b>NCA</b>	National Communications Authority
<b>ECG</b>	Electricity Company of Ghana	<b>NCA-CERT</b>	National Communications Authority- Cyber Emergency Response Team
<b>EOCO</b>	Economic and Organised Crime Office	<b>NCC</b>	National Cybersecurity Challenge
<b>E-Crime Bureau</b>	Economic Crime Bureau	<b>NCCE</b>	National Commission for Civil Education
<b>ETL</b>	Extract, Transform, Load	<b>NCSAM</b>	National Cyber Security Awareness Month
<b>FIC</b>	Financial Intelligence Bureau	<b>NCSC</b>	National Cyber Security Centre
<b>FIRST</b>	Forum of Incident Response and Security Teams	<b>NCSS</b>	National Cyber Security Secretariat
<b>GAB</b>	Ghana Association of Bankers	<b>NCSTWG</b>	National Cyber Security Technical Working Group
<b>GAF</b>	Ghana Armed Forces	<b>NIA</b>	National Identification Authority
<b>GARNET</b>	Ghanaian Academic and Research Network	<b>NIB</b>	National Intelligence Bureau
<b>GCI</b>	Global Cybersecurity Index	<b>NITA</b>	National Information Technology Agency
<b>GCSCC</b>	Global Cyber Security Capacity Centre	<b>NPA</b>	National Petroleum Authority
<b>GCTU</b>	Ghana Communications Technology University	<b>NPRA</b>	National Pensions Regulatory Authority
<b>GC3B</b>	Global Conference on Cyber Capacity Building	<b>NSB</b>	National Signals Bureau
<b>GDNr</b>	Ghana Domain Name Registry	<b>OCSEA</b>	Online Child Sexual Exploitation and Abuse
<b>GIZ</b>	Deutsche Gesellschaft für Internationale Zusammenarbeit	<b>OCWAR-C</b>	Organised Crime West African Response to Cybersecurity and fight against Cybercrime
<b>GJA</b>	Ghana Journalists' Association	<b>PCA</b>	Private Cloud Appliance
<b>GLACY+</b>	Global Action on Cyber Crime Extended	<b>PoC</b>	Point of Contact
<b>GMA</b>	Ghana Maritime Authority	<b>PPP</b>	Public Private Partnerships
<b>GNAT</b>	Ghana National Association of Teachers	<b>RD</b>	Research Department
		<b>SIGA</b>	State Interest and Governance Authority
		<b>SOEs</b>	State-Owned Enterprises
		<b>TAIEX</b>	Technical Assistance and Information Exchange Instrument
		<b>UNICEF</b>	United Nations International Children's Emergency Fund
		<b>UNODC</b>	United Nations Office on Drugs and Crime
		<b>VCG</b>	Vice Chancellors of Ghana
		<b>VPN</b>	Virtual Private Network
		<b>Wi-Fi</b>	Wireless Fidelity

# Executive Summary

October has been internationally recognised as Cyber Security Awareness Month since 2003. Ghana joins the rest of the world yearly to mark the celebration and has adopted it as the National Cyber Security Awareness Month (NCSAM). In Ghana, the Cyber Security Authority (CSA) is mandated to organise the yearly event by promoting awareness and understanding of cybersecurity issues with a focus on Children, the Public, Businesses and Government.

The NCSAM 2023 theme, ***“Promoting a Culture of Digital Safety,”*** centred on the essence of promoting a culture of cybersecurity among Ghanaians in general, addressing the consequences of unsafe digital practices, improving collaboration among stakeholders, and equipping the populace with the necessary skills to help combat cybercrimes.

The launch of the celebration on October 2, 2023, at the College of Physicians and Surgeons in Accra marked the commencement of a series of activities planned to commemorate the occasion.

Following the launch, there were workshops and seminars with different industry stakeholders including registered Cybersecurity Professionals, Establishments, and Service Providers. These gatherings focused on discussing issues related to the licensing and accreditation process, which commenced on March 1, 2023, among others.

Furthermore, there were collaborative awareness creation events between the Cyber Security Authority (CSA) and various institutions including member institutions of the Joint Cybersecurity Committee (JCC) and the Joint Intelligence Committee (JIC). These collaborations were highly effective in raising awareness about cybersecurity across different sectors.

Moreso, attention was given to fostering cybersecurity awareness among children through the National Cybersecurity Challenge (NCC). This initiative, which was integrated into the National Cybersecurity Awareness Month (NCSAM) activities the previous year, garnered substantial support and enthusiasm from Ghanaians nationwide, particularly among online viewers. Building on the success and memorable moments of the inaugural edition, this year's NCC witnessed remarkable participation, with contestants displaying a strong desire to excel. Ultimately, OLA Girls' Senior High School emerged as the champion, earning a prestigious “bragging right”.

There were many stakeholder-organised events for their constituents with the support of the CSA and hence increasing awareness, encouraging partnerships, showcasing innovations, advocating for legislative changes, and measuring impact. Several stakeholder-organised events were conducted for respective constituents, with the support of the CSA, achieving its aim to heighten awareness, foster partnerships, highlight innovations, advocate for legislative changes, and assess the overall impact of cybersecurity initiatives.

The following are some selected events held to achieve the objectives of the NCSAM:

- Benefits of Sectoral CERT Accreditation
- Introductory Course on Cybercrime and Electronic Evidence for Judges and Prosecutors in Ghana
- Engagements with registered Cybersecurity Service Providers, Establishments and Professionals
- Workshop on the Protection of Critical Information Infrastructure
- National Cyber Drill on Incident Response

# National Cybersecurity Leadership



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



**DR. ALHAJI MAHAMUDU BAWUMIA**  
Vice President of the Republic of Ghana



**HON. MRS. URSULA OWUSU-EKUFUL**  
Minister for Communications and Digitalisation



**HON. AMA POMAA BOATENG**  
Deputy Minister for Communications  
and Digitalisation



**DR. ALBERT ANTWI-BOASIAKO**  
Director-General, Cyber Security Authority

# Overview of the Cybersecurity Act, 2020 (Act 1038)









## Mandate of the CSA



# Institutional Framework



# CSA Governing Board



**HON. MRS. URSULA OWUSU-EKUFUL**  
Minister for Communications and Digitalisation  
(Chairperson)



**HON. ALBERT KAN-DAPAAH**  
Minister for National Security



**HON. AMBROSE DERY**  
Minister for the Interior



**HON. DOMINIC NITIWUL**  
Minister for Defence



**DR. ALBERT ANTWI-BOASIAKO**  
Director-General, Cyber Security Authority



**AMB. ESTHER DZIFA OFORI**  
President's Representative



**MRS. MAVIS VIJAYA AFAKOR AMOA**  
President's Representative



**MRS. ADELAIDE BENNEH-PREMPEH**  
President's Representative



**PROF. BOATENG ONWONA-AGYEMAN**  
Industry Forum



**MR. CARL A. SACKEY**  
Industry Forum



**MR. REGINALD BOTCHWEY**  
Industry Forum

# Joint Cybersecurity Committee



**DR. ALBERT  
ANTWI-BOASIAKO**  
Director-General, CSA



**JUSTICE AFIA  
SERWAH ASARE-BOTWE**  
Superior Court of Judicature



**MR. RICHARD OKYERE-FOSU**  
Director-General, NITA



**MR. JOE ANOKYE**  
Director-General, NCA



**MS. PATRICIA ADUSEI-POKU**  
Executive Director, DPC



**DR. MAXWELL OPOKU-AFARI**  
First Deputy Governor, BoG



**MR. KWAKU DUA**  
Chief Executive Officer, FIC



**NANA ATTOBRAH QUACO**  
Ag. Director-General, NIB



**COP. MAAME YAA  
TIWAA ADDO-DANQUAH**  
Executive Director, EOCO



**DCOP. MR. FREDERICK AGYEI**  
Deputy Director-General, CID



**COL. (DR) TIM BA-TAA-BANAH**  
Director, NCTFC



**MR. KWABENA ADU-BOAHENE**  
Director-General, NSB



**MAJ. GEN. A. Y. NSIAH**  
Chief of Defence Intelligence, DI



**MR. LAUD  
AKWASI AFFRIFAH**  
Deputy Comptroller-General, GIS



**AMB. GEORGE ABAKA  
BLANKSON**  
Deputy Director-General, RD



**COL. A. K. ODUAH**  
Ag. Director-General (DCIS), GAF



**MS. YVONNE  
ATAKORA OBUOBISA**  
Director of Public Prosecutions



**NANA  
KOFI ASAFU-AIDOO**  
Executive Director, GDNR



## Overview of the 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 October 1, 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.

## Core Values



**Confidentiality**



**Inclusiveness**



**Integrity**



**Commitment**



**Reliability**



**Professionalism**



### Vision

To ensure a Secure and Resilient Digital Ghana.



### Mission

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

# 01.

**Media Launch of the  
National Cyber Security  
Awareness Month (NCSAM) 2023**





# MEDIA LAUNCH OF THE NATIONAL CYBER SECURITY AWARENESS MONTH (NCSAM) 2023



**Hon. Fatimatu Abubakar**  
Deputy Minister for Information

## Opening Remarks

**Hon. Fatimatu Abubakar**  
Deputy Minister for Information

Hon. Fatimatu Abubakar, who moderated the event, welcomed guests to the media launch and stated that the event was critical in ensuring that all Ghanaians participated in the National Cyber Security Awareness Month. She added that awareness creation was key to ensuring that everyone who used the internet had a safe experience.

## Address

**Hon. Ama Pomaa Boateng**  
Deputy Minister for Communications & Digitalisation

The Deputy Minister for Communications and Digitalisation, Hon. Ama Pomaa Boateng, noted that several nations, including Ghana, have designated October as a month to promote awareness of digital security and to empower the public, businesses, and

government to protect essential data considering the ever-changing global digital threats.

She revealed that the 2023 NCSAM was intended to further bridge the gap between private and public stakeholder groups to raise awareness about the importance of cybersecurity.



**Hon. Ama Pomaa Boateng**  
Deputy Minister for Communications & Digitalisation

She indicated that the media launch was an important part of preparing for NCSAM 2023, which was intended to address workplace concerns by raising cybersecurity awareness in institutions.

Hon. Boateng consequently urged the media to assist in educating the public on issues related to internet safety adding that the media launch should foster cross-sector collaboration to enhance the impact of digital safety ahead of NCSAM 2023.



## Presentation

**Dr. Albert Antwi-Boasiako**

Director-General, Cyber Security Authority

The Director General of the Cyber Security Authority, Dr. Albert Antwi-Boasiako, noted that although Ghana had made a lot of progress in creating public awareness on cybersecurity issues, there was the need to intensify awareness creation amongst the youth especially, as they practically live online.

He announced that the Authority received 41,285 contacts from the public between October 2019 and July 2023 with 41 percent of the issues the callers raised relating to online fraud, including shopping fraud, romance fraud, online blackmail, and identity fraud. He indicated the need for collective efforts to secure digital safety and charged individuals to take personal responsibility for protecting themselves against digital fraud.

Dr. Antwi-Boasiako further called for institutional harmonisation and integration of the work of state agencies in collating statistics on arrests, prosecutions, and convictions of persons involved in cyber fraud and cybercrimes.

He observed that global digitalisation trends had changed the way businesses operated adding that “the government is creating opportunities and enabling interventions for economic growth.”

The Director-General averred that the theme for NCSAM 2023 highlighted the importance of cultivating a collective mindset and behaviour that valued and promoted responsible online practices, cybersecurity awareness, and the protection of personal information.

“We expect this media launch to set in motion a month-long national cybersecurity awareness creation that will assemble public and private sector players, cybersecurity professionals, the academia, and representatives from civil society organisations, in preparation for the NCSAM as we seek to encourage every Ghanaian to stay digitally alert,” he stressed.

He called for collaborative efforts to harmonise the processes of public procurement in the public service to secure a judicious, economic, and efficient use of state resources and provide a streamlined mechanism for guaranteeing that cybersecurity service providers, establishments, and professionals in the country executed their duties according to approved international standards.



## Remarks

**Dr. Kenneth Ashigbey**

Chief Executive Officer, Ghana Chamber of Telecommunications.

Dr. Kenneth Ashigbey, Chief Executive Officer of the Ghana Chamber of Telecommunications, noted that the public owed it to themselves to take cyber hygiene seriously, describing the 2023 theme as apt considering the current times.

According to him, the Chamber of Telecommunication had already taken steps to conduct cybersecurity awareness programmes for its employees and asked institutions affiliated with the Chamber to participate actively in NCSAM 2023.



**John Awuah**  
CEO of the Ghana Association of Banks

## Remarks

**John Awuah**  
CEO of the Ghana Association of Banks

Emphasising the importance of online activities, Mr. Awuah, CEO of the Ghana Association of Banks, noted that the days of going to banks to apply for loans and obtain ATM cards, among other financial services, were long gone due to the convenience of digitalisation. "We are moving forward in the digital journey," he added and urged the country's financial institutions to take cyber awareness seriously. "We all must protect each other, and it is only when we know we are doing the right thing that we can ensure that everyone is secure," he said.



**Albert Kwabena Dwumfour**  
President, Ghana Journalists' Association (GJA)

## Remarks

**Albert Kwabena Dwumfour**  
President, Ghana Journalists' Association (GJA)

Mr. Dwumfour described the theme "Promoting a Culture of Digital Safety" as extremely important given the alarming rate of cyber-attacks across Africa. He acknowledged that digitalisation was preparing the world for rapid development adding that the complete impact of digitalisation could not be realised without the protection of the online space including businesses. He lauded the CSA for initiating the annual NCSAM and expressed the belief that the initiative was key to educating the public on the significance of digital safety.

He called on the CSA to hold sensitisation workshops to empower the media and encourage them to take an interest in cybersecurity reporting.

Mr. Dwumfour pledged the support of the media fraternity to ensure the objectives of NCSAM are realised.





**Carl Sackey**  
Member of the CSA Governing Board

## Remarks

**Carl Sackey**  
Member of the CSA Governing Board

Speaking on behalf of the Governing Board, Mr. Carl Sackey said that the theme for NCSAM 2023 underlined the necessity of the collective action of Ghanaians to

safeguard the country's digital assets, intellectual property, and the confidential information of citizens.

He added that it was important to consider education, transparency and accountability, regular system updates and drills, and legislation as some key building blocks for a culture of digital safety.

According to Mr. Sackey, achieving this mission was not the responsibility of a few but the collective duty of all.

## Conclusion

Hon. Fatimatu Abubakar, the Deputy Minister for Information gave the concluding remarks as she urged the public to participate in the 2023 celebration of NCSAM.



# 02.

**Official Launch of the 2023 Edition  
of the National Cyber Security  
Awareness Month  
(Promoting a Culture of Digital  
Safety)**



# OFFICIAL LAUNCH OF THE 2023 EDITION OF THE NATIONAL CYBER SECURITY AWARENESS MONTH

## Background

The 2023 edition of the National Cyber Security Awareness Month (NCSAM) sought to highlight the importance of cultivating a collective mindset and behaviour that values and promotes responsible online practices, cybersecurity awareness, and the protection of personal information.

The month-long programme on the theme, “Promoting a Culture of Digital Safety,” was officially launched on Monday, October 2, 2023, at the College of Physicians and Surgeons in Accra. In attendance were Ministers of State, Members of the CSA Governing Board, Members of Parliament, Members of the Joint Cybersecurity Committee (JCC) and the Joint Intelligence Committee (JIC), Ambassadors and High-Commissioners, Heads of agencies and institutions, industry players, academia, and the media.

## Welcome Remarks

**Dr. Albert Antwi-Boasiako**

Director-General, Cyber Security Authority

Welcoming the audience to the official launch of the month-long programme, the Director-General of the CSA, Dr. Albert Antwi-Boasiako, indicated that cybersecurity development is very important due to the fast-evolving nature of cybercrimes. He further noted that “cybercrime comes in many forms, with the human element considered the weakest link – both for cyber dependent and cyber-enabled crimes, noting that with a click of a button, malicious actors can now carry out cyberattacks that drastically affect the citizenry, businesses, and governments.”

According to Dr. Antwi-Boasiako, the economic development of the African continent has brought about an increase in the demand for the Internet and other digital services and solutions. This, in turn, has



introduced the continent to benefits and opportunities, as well as challenges. He announced that from January to September 2023, the National Computer Emergency Response Team (CERT-GH) recorded 9,296 reports through its Cybercrime/Cybersecurity Incident Points of Contact (PoC) and top among the incidents reported were cyberbullying, online fraud, online blackmail, unauthorised access, and online impersonation, all of which have led to a total of 49.5 million Ghana Cedis in monetary losses as of June 2023.

Dr. Antwi-Boasiako noted that cybersecurity awareness is vital in improving the nation's security and building a resilient digital economy, adding that this year's theme was vital to ensuring that the country is digitally safe with a collective mindset and behaviour that encouraged and promoted cybersecurity best practices among Children, the Public, Businesses, and the Government.



He said as a regulatory body, the CSA, could only be proactive and lead national response through the implementation of regulatory interventions such as the licensing of Cybersecurity Service Providers (CSPs), Accreditation of Cybersecurity Establishments (CEs) and Cybersecurity Professionals (CPs), which allow for the first time in history, a record of such establishments and professionals in Ghana.

Dr. Antwi-Boasiako entreated the public to actively participate in the NCSAM celebration, noting that the “Authority has an unobstructed vision and focus to develop Ghana’s cybersecurity and that awareness creation towards promoting a culture of digital safety.”



**Dr. Patrick Awuah**  
President of Ashesi University

## Remarks

**Dr. Patrick Awuah**  
President of Ashesi University

Focusing on the intrusions of malicious actors in the cyberspace, Dr. Awuah shared several examples of how otherwise complex computer systems have been compromised, noting that incidents would always occur, but the difference is in the nature and timing of responses. He called for the adoption of a holistic mindset to ensure effective response to cyber threats. He further noted that education ensures good cybersecurity practices, urging institutions to train their staff as end-users regularly.

Dr. Awuah additionally recommended that institutions be open to internship programmes for young talents to adequately close the current cybersecurity talent gap.



**Fiachra McAsey**  
Deputy Country Representative of UNICEF

## Address

**Fiachra McAsey**  
Deputy Country Representative of UNICEF

Mr. Fiachra McAsey commended the CSA for efforts in strengthening the nation’s cyber security and for

hosting the NCSAM annually. He noted the importance of the internet and its prevalence in the daily lives of citizens, especially among children and the alarming statistics of crimes affecting children specifically, issues of online sexual exploitation and abuse. Mr. McAsey enumerated UNICEF's collaboration with the CSA in the development of a Legislative Instrument for the Cybersecurity Act, 2020 (Act 1038) and a Child Online Protection Framework.

He further mentioned the awareness and sensitisation of cybersecurity issues in Senior High Schools that has led to the introduction of the annual National Cybersecurity Challenge (NCC). To achieve a culture of digital safety, Mr. McAsey argued that all hands were needed on deck as he pledged UNICEF's commitment to the protection of children online.

## Address

**Hon. Albert Kan-Dapaah**

Minister for National Security

Hon. Albert Kan-Dapaah described the fast-paced nature of Africa's internet connectivity as a double-edged sword that creates developmental opportunities and at the same time presents security threats.

He emphasised the urgency of fostering a culture of digital safety as an investment in that area, noting that it empowered individuals to navigate the online world safely. He made a case for investments in robust cybersecurity measures to protect critical infrastructure, data, and government networks. The minister underscored the need for a cyber-defence capability to respond swiftly and decisively to cyber threats and called on relevant institutions to prioritise digital literacy, promote public awareness campaigns on cyber security and adopt secure practices.

"I appreciate the works of the CSA in securing a safer digital nation. Let us all join hands in raising



awareness because this can be achieved through mass communication and education," Hon. Kan-Dapaah added.

## Keynote Address

**Moctar Yedaly**

Special Envoy of the Global Conference on Cybersecurity Capacity Building (GC3B)

Delivering the keynote address, the Special Envoy for the Global Conference on Cyber Capacity Building (GC3B), Mr Moctar Yedaly, reiterated the alarming rise of cyber threats and crimes in the digital age. He noted that promoting a culture of digital safety was important for citizens and organisations, especially on the African continent, emphasising that Ghana is a beacon of leadership in cybersecurity capacity building not in only Africa but also the world. Referencing the vision of Osagyefo Dr. Kwame Nkrumah, Ghana's first President, Mr



**Moctar Yedaly**  
Special Envoy of the Global Conference on Cybersecurity  
Capacity Building (GC3B)

Yedaly entreated the public to take on a unified collaborative approach to tackling cybersecurity on the continent, noting that there is a need to work persistently to guarantee and promote a culture of digital safety for everybody.

## Official Launch

**Hon. Ama Pomaa Boateng**

Deputy Minister for Communications and Digitalisation

The Deputy Minister for Communications and Digitalisation, Hon. Ama Pomaa Boateng, who represented the sector Minister, Hon. Ursula Owusu-Ekuful, in launching the NCSAM 2023 emphasised that the rapidly evolving cybersecurity industry presented Ghana with increased opportunities and challenges, stressing that the growth of Ghana's cybersecurity development through the efforts of the CSA such as the ratification of relevant international conventions, the designation of Critical Information Infrastructures



**Hon. Ama Pomaa Boateng**  
Deputy Minister for Communications and Digitalisation

(CII), the institutionalisation of cybersecurity to foster regional cooperation, and efforts to strengthen international cooperation through the signing of memorandum of understanding with Mozambique and Rwanda were exemplary.

She encouraged individuals and organisations to "keep in mind that the impact of our actions reaches far beyond our individual lives", and urged the public to take cybersecurity issues seriously to protect their personal interests and the broader security and stability of society.

## Conclusion

The Executive Director of the Ghana Domain Name Registry and member of the JCC, Nana Kofi Asafu-Aidoo, in a vote of thanks, appreciated Hon. Mrs Ursula Owusu-Ekuful, for her dedication over the years to the development of cybersecurity. He also extended appreciation to the media, partners, and sponsors.

# 03.

**Joint Cybersecurity  
Committee (JCC) / Joint  
Intelligence Committee  
(JIC) Related Events**





# LAUNCH OF CYBER SECURITY AWARENESS MONTH FOR THE PERSONNEL OF THE GHANA ARMED FORCES

## Background

The Ghana Armed Forces (GAF), which is represented on the Joint Cybersecurity Committee (JCC) launched for a second time in a row, Cybersecurity Awareness Month for its service men and women at the Burma Hall, Burma Camp in Accra on September 29, 2023, in collaboration with the Defence Intelligence (DI), which is also a member institution of the JCC. The event was organised as part of internal efforts to promote cyber security consciousness and to equip personnel of the GAF and DI with the requisite competencies to ensure cyber hygiene within the military.

In attendance were the Director-General of the CSA, Dr. Albert Antwi-Boasiako, the Executive Director of the Data Protection Commission, Madam Patricia Adusei-Poku, the Chief of Defence Staff of the Ghana Armed Force, Vice Admiral Seth Amoama, personnel of the GAF and other dignitaries.

## Opening Remarks

**Colonel Elikem Fiamavle**

Department of Defence, Communication, and Information Systems

Colonel Fiamavle, in his opening remarks, indicated that the month-long event was a period used by the Department of Defence, Communication, and Information Systems of the GAF to raise awareness and educate all ranks within the force, their families, and the populace about Cybersecurity related issues. That, he explained was necessary as the GAF was designated as a Critical Information Infrastructure (CII).



**Colonel Elikem Fiamavle**  
Department of Defence, Communication, and Information Systems

To achieve this, he stated that the department would adopt the use of lectures and weekly seculars which would be published on the website of the GAF to give tips on good cyber practices.

He further pointed out that in as much as the internet was a wide and free space, there were criminal implications for its wrongful use such as forgery, fraudulent electronic transactions, and the use of illegal devices as provided by sections 107-140 of the Electronic Transactions Act 2008 (Act 772).

## Address

**Patricia Adusei-Poku**

Executive Director of the Data Protection Commission (DPC)

Madam Adusei-Poku's remarks centred on the role of data protection in cybersecurity, indicating that the ultimate subject of cybersecurity was data and its protection.

She explained that data, being the new oil, can be mined and used for business and social purposes and thus the need for its protection by all.



**Patricia Adusei-Poku**  
Executive Director of the Data Protection Commission (DPC)

She encouraged participants to make use of the data protection law, which empowers citizens to have a say and to protect themselves from unauthorised use of their data.



**Dr. Albert Antwi-Boasiako**  
Director-General of the CSA

## Remarks

**Dr. Albert Antwi-Boasiako**  
Director-General of the CSA

Dr. Albert Antwi-Boasiako, the Director-General of the CSA set the tone by commending the GAF for pioneering the celebration of NCSAM by JCC

member institutions in 2022. He noted that more than 10 of the 18 JCC member institutions had joined in organising activities to mark the celebrations of NCSAM 2023.

Dr. Antwi-Boasiako shared reflections on the vision of the CSA, which is to work with all stakeholders to achieve the vision of becoming number one in Africa and among the top 25 in the world in the Global Cybersecurity Index.

Dr. Antwi-Boasiako explained that to promote a culture of digital safety means that individually, “we need to adopt cyber hygiene practices and further educate family members and colleagues to adopt same.”



**Vice Admiral Seth Amoama**  
Chief of Defence Staff of the GAF

## Keynote Address

**Vice Admiral Seth Amoama**  
Chief of Defence Staff of the GAF

Vice Admiral Seth Amoama said the GAF joined other institutions of the JCC to mark NCSAM to intensify capacity-building and awareness-creation efforts on cybersecurity and cybercrime by educating the public on the importance of promoting a culture of digital safety.

He added that the domain of cyber had added up to the traditional domains of land, sea, air, and space, hence the dedication to its protection, noting that



terrorists and other violent extremist groups were using the internet as platforms to further their activities.

To this end, he stressed that cybersecurity has therefore become a vital part of the operational effectiveness of militaries around the world.

He further indicated that the GAF was making conscious efforts to sensitise its officers to appreciate the nuances associated with cyber threats, vulnerabilities, their impact, and the nation's readiness to combat them.

Vice Admiral Amoama intimated that the GAF had the responsibility to protect the data, databases, and networks of the GAF and the country, and that to ensure the efficient safeguarding of information

systems and computer networks, the safety of data transmission, and the security of internet users, it was imperative to acknowledge the significance of fostering a cybersecurity culture.

He announced that plans were afoot to establish a directorate for cybersecurity for the GAF, and concluded by encouraging personnel to uphold the good image of the GAF by becoming cybersecurity conscious; being mindful of what to share, when and where to share information on the internet.

Launching the NCSAM 2023 for the GAF, Vice Admiral Amoama urged his officers and men to adhere to data protection practices which were critical to Ghana's digitalisation agenda.

## WORKSHOP ON CYBERSECURITY SENSITISATION FOR STAFF OF THE FINANCIAL INTELLIGENCE CENTRE (FIC)

### Background

The CSA collaborated with the Financial Intelligence Centre (FIC), a member-institution of the Joint Cybersecurity Committee (JCC) to organise a cybersecurity sensitisation event for their staff and stakeholders as part of the NCSAM.

About 35 participants were in attendance including the CEO of the FIC, Mr. Kwaku Dua; the Director-General of the National Information Technology Agency (NITA), Mr Richard Okyere-Fosu; the Director-General of Defence Intelligence, Major General A.Y. Nsiah; the acting Director of Capacity Building and Awareness Creation at the CSA, Mr Alexander Oppong, and staff members of the FIC and the CSA.

The workshop was aimed at cybersecurity consciousness among the participants.

### Opening Remarks

**Kwaku Dua**  
CEO of the FIC

Mr. Kwaku Dua acknowledged the rapidly evolving digital landscape in which the country operates, emphasising that Ghana has experienced significant digital transformation. He indicated that despite the unprecedented opportunities presented by the digital age, there are also challenges and risks.

He stated that the mission of the FIC was to protect the integrity of Ghana's financial system by detecting and preventing money laundering and terrorist financing activities. He added that the FIC in 2019, recorded up to US\$ 45.2 million as a total sum of suspicious inflows of cash into the country and of the amount, US\$ 40 million was connected to cybercrime



**Kwaku Dua**  
CEO of the FIC

activities such as romance fraud and business email compromise.

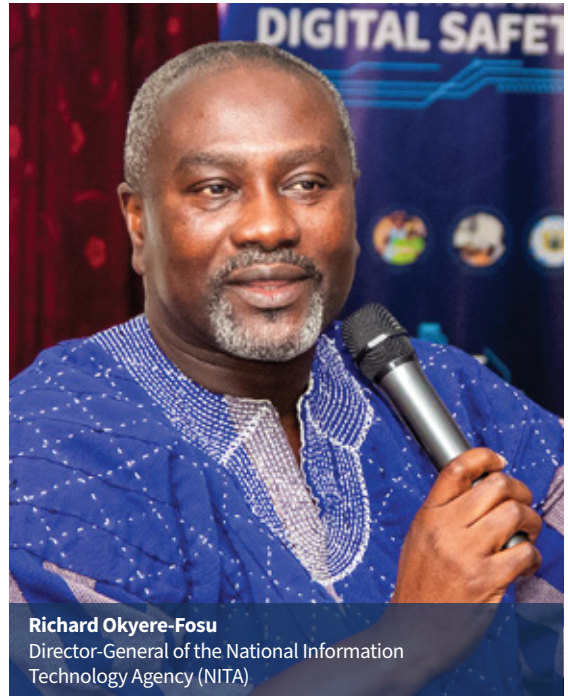
Similarly, he said, in 2020 and 2021, the FIC recorded US\$ 4.7 million and US\$ 1.8 million respectively being the total sum of suspicious cyber-related inflows to Ghana. “It is imperative that as individuals we take steps to ensure our nation’s digital ecosystem remains robust, resilient and protected against cyber threats,” he added.

## Address

**Richard Okyere-Fosu**

Director-General of the National Information Technology Agency (NITA)

Mr. Richard Okyere-Fosu stated that the FIC was a potential target for cyberattacks because of its mandate to protect the integrity of Ghana’s financial system by detecting and preventing money laundering and terrorist financing activities and also due to the volume of sensitive information in its possession.



**Richard Okyere-Fosu**  
Director-General of the National Information Technology Agency (NITA)

He added that the rise in Ghana’s fintech industry, spurred on by the government’s digitalisation agenda had increased the scope of potential attacks and threats in the financial ecosystem.

Highlighting relevant statistics to buttress his point, Mr. Okyere-Fosu stated that the United Nations Office on Drugs and Crime (UNODC) estimated that between 2% and 5% of the global GDP (Euros 715 billion and 1.8 trillion) was laundered each year. He indicated that Ghana aimed to have a cashless and contactless digital economy while enhancing financial inclusion and stability. “It is therefore important that collaboration is maintained to ensure a strong focus on cybersecurity awareness and its best practices”.

## Presentation

**Kwaku Acheampong**

Cybersecurity Analyst, FIC

In furtherance to presentations made on the mandate of the FIC, a Cybersecurity Analyst of the institution, Mr. Kwaku Acheampong, in a



**Kwaku Acheampong**  
Cybersecurity Analyst, FIC

presentation focused on Cyber Risk and Incident Reporting, delved into the risks and potential harm associated with the use of technological devices.

Highlighting the significance of proactive measures, Mr. Acheampong underscored the importance of institutions establishing a Cybersecurity Incident Response Team. Such a team, he emphasised, plays a crucial role in swiftly detecting and responding to incidents, ensuring a practical and immediate response to potential cybersecurity threats.

## Conclusion

Participants gained in-depth knowledge of the mandate of the FIC concerning cybersecurity. Referencing data from the International Business Machines (IBM), which indicates that human error is responsible for 90% of all cyber breaches, participants were urged to be cybersecurity-conscious.

# SENSITISATION WORKSHOP ON DATA PROTECTION

## Background

As part of the special initiatives and collaborative events between the CSA and institutions on the JCC, the DPC held a Data Protection and Cyber Security Sensitisation Engagement on October 12, 2023.

## Opening Remarks

**Alexander Oppong**

Acting Director for Capacity Building and Awareness Creation, CSA

Mr. Oppong, representing the Director-General of the CSA, Dr. Albert Antwi-Boasiako, expressed gratitude to the DPC under the leadership of Madam Patricia Adusei-Poku for undertaking the initiative to hold the activity as part of the National Cyber Security Awareness Month.

He noted that October is recognised by several countries worldwide as a dedicated period for raising awareness on cybersecurity, cyber threats and attacks, as well as promoting cybersecurity best practices. He indicated that the theme for the 2023 edition of the NCSAM, "Promoting a Culture of Digital Safety", aims at highlighting the importance of cultivating responsible cyber hygiene practices, and the protection of personal information.

Mr. Oppong referenced statistics from the national Computer Emergency Response Team (CERT GH) of the CSA, revealing that from January to September 2023, the Cybersecurity/Cybercrime incident reporting points of contact at the CSA received 9,296 contacts. Of these, 870 (representing 9%) were categorised as actual cyber-related incidents, and 8,426 (representing 91%) were categorised as direct

advisories. The advisories were issued to citizens seeking to fact-check information they had encountered online before taking certain actions online.

He emphasised that in digital safety, regulators have a duty to empower the public by encouraging proper and responsible technology use and the protection of personal data. Mr. Oppong expressed confidence that the CSA and the DPC could collaborate to safeguard all types of data against theft and loss, especially critical information infrastructure.

He subsequently highlighted Ghana's significant progress in the technological sphere, ranking 4th in Africa with a score of 51.4% and substantial improvements in connectivity over the last five years, according to the Group Special Mobile Association Mobile Connectivity Index 2023 report. He mentioned that Ghana scored 86.69% in online security, a key dimension of the index consistent with the country's score on the Global Cybersecurity Index (GCI) of the International Telecommunication Union.

Mr. Oppong emphasised that these developments reaffirmed Ghana's cybersecurity readiness, underscoring the need to educate individuals on keeping themselves and their data safe in the digital space.

## Address

**Patricia Adusei-Poku**  
Executive Director, DPC

Ms. Patricia Adusei-Poku expressed her appreciation for the opportunity to collaborate with the CSA to educate Ghanaians and improve their level of awareness and knowledge of cybersecurity and data protection. She added that the collaboration had established a better understanding of the connection between the regulatory mandates of the two institutions in relation to their overlapping roles and helped data subjects understand where to address their issues and escalate their matters when the need arises.

She said the DPC was ready to engage with other state actors to provide an overview of what data

protection entails and its connection with cybersecurity.

## Sensitisation

**Quintin Akrobotu**

Director of Regulation and Compliance, DPC

Mr. Quintin Akrobotu delivered a presentation on practising responsible digital behaviour, "Why should we be concerned about cybersecurity?" He asserted the importance of responsible digital behaviour and how it impacts preserving and securing privacy and personal information.

Mr. Akrobotu underscored the consequences of not engaging in appropriate digital activities, emphasizing the vulnerability of servers and the potential promotion of anti-money laundering, which can impact negatively on individuals, the government, and the nation. His presentation delved into prevalent cyber risks such as phishing, malware, ransomware, social engineering, and identity theft. He then outlined fundamental principles for responsible digital behaviour, including the use of strong passwords, multi-factor or two-factor authentication, regular software and security upgrades, safe browsing practices, data backups, privacy settings management, and the reporting of suspicious activities.

## Presentation

**Hilda Odua Sowah**

Head of Accreditation and Training, DPC

Ms. Hilda Odua Sowah's presentation was on addressing breach notifications, defining a data breach as any security incident resulting in unauthorised access to confidential information. She elaborated on the concept of data breach notifications, emphasising the process of informing customers and other relevant parties about data breaches and taking specific remedial actions in accordance with jurisdictional and regulatory requirements.



Ms. Sowah pointed out that the Data Protection Act, 2012 (Act 843), specifically in section 37, outlines the procedures for reporting a data breach to the Data Protection Commission (DPC). Additionally, she highlighted Sections 47 and 48 of the Cybersecurity Act 2020 (Act 1038), which detail the prescribed responses and notification procedures to be followed by the Cyber Security Authority (CSA) and data controllers in the event of a data breach.

## Conclusion and Recommendations

Concluding the session, Ms. Natasha Hammond noted that the participants had demonstrated keen interest in data protection and cybersecurity. She expressed hope that the most effective strategy for countering cyber threats lay in the public's unity, emphasizing the importance of a collective effort to combat cybercrime.

# LAUNCH OF THE NATIONAL CYBERSECURITY AWARENESS MONTH BY NATIONAL SIGNALS BUREAU

## Background

To achieve the goal of NCSAM 2023 by promoting a culture of digital safety, the National Signals Bureau (NSB) in collaboration with the CSA organised an internal launch of the NCSAM for their staff and stakeholders to outline their programme of activities for NCSAM 2023.

The event which took place at the NSB Head Office in Accra on October 11, 2023, was attended by the Director-General of the NSB, Mr Kwabena Adu-Boahene; the acting Director, Capacity Building and Awareness Creation at the CSA, Mr. Alexander Oppong, Directors of the NSB, and staff of both the CSA and NSB.

## Opening Remark

**Evelyn Aniagyei**

Director of Administration, NSB

Madam Evelyn Aniagyei in her remarks extended a warm welcome to all participants present at the launch of the NSB NCSAM 2023, noting that the mission of the NSB includes securing the cyberspace of the country and collaborating with institutions to foster a resilient cyberspace.

She indicated that internal cybersecurity training was a requirement for staff of the NSB to be abreast of cybersecurity matters.

Madam Aniagyei concluded that the NSB was observing Cyber Security Awareness Month as part of internal efforts to promote cybersecurity consciousness and to provide staff with the knowledge and skills necessary to ensure cyber hygiene which will have a cascading effect on their families. She added that activities were planned for the entire month of October along with the nationwide activities being organised by the Cyber Security Authority.

## Presentation

**Gifty Selby**

Director for Communications Networks for the NSB

Madam Gifty Selby in her presentation noted that the NSB's participation in awareness creation during the 2023 NCSAM is very critical as they will be creating cybersecurity awareness for their staff and their stakeholders. She described as relevant the 2023 NCSAM theme "Promoting a culture of digital safety" given the benefits that come with the rapid growth of digitalisation and the related threats.

She pledged the support of the NSB towards the awareness creation efforts to enhance the cyber resilience of Ghana.



**John Tandoh**

Director of Cyber Information Assurance, NSB

## Presentation

**John Tandoh**

Director of Cyber Information Assurance, NSB

In his presentation, Mr. John Tandoh outlined the NSB's plan for the National Cyber Security Awareness Month, which included daily cybersecurity training sessions for staff throughout the month.

He mentioned that the NSB is set to host a roundtable discussion involving seventeen Information Technology (IT) unit heads from different government agencies that the NSB works

with. He further stated that the Bureau would be conducting specialised training sessions for two selected agencies they collaborate with, and further shared the curriculum for the cybersecurity training of staff which encompasses a range of topics such as an introduction to cybersecurity, understanding cyber threat actors, recognising social engineering, and the perils of phishing. Mr. Tandoh noted that training sessions would incorporate practical demonstrations, address password security with hands-on examples, delve into the safety of public networks, and emphasise the importance of data backups.

With respect to the roundtable discussion among IT heads, Mr Tandoh stated that the agenda would revolve around collaboration, preparedness for incidents beyond Ghana's borders, awareness creation, policy development to establish security and intelligence agency standards, incident response strategies, cybersecurity resource allocation, and capacity building efforts.

Mr. Tandoh also mentioned the significance of agency training, which aims at enhancing knowledge, reducing vulnerabilities, improving response capabilities, ensuring consistent compliance with cybersecurity measures, mitigating risks, fostering inter-agency cooperation, handling sensitive information, and addressing the human factor or human firewall in the context of cybersecurity.

## Address

**Alexander Oppong**

Acting Director of Capacity Building and Awareness Creation, CSA

Mr. Alexander Oppong commenced by conveying the appreciation and gratitude of the Director-General of the CSA for the ongoing support extended by the NSB to the CSA as a member of the JCC. He proceeded to provide insights into the incidents reported to the National Computer Emergency Response Team of the CSA through the Points of Contacts (POC), noting that from January to September 2023, the CSA received a total of 9,296 contacts via its Cybercrime/Cybersecurity Incidents Points of Contact (PoC). The predominant incident categories reported were Cyber Bullying (36%), primarily

**Alexander Oppong**

Acting Director of Capacity Building and Awareness Creation, CSA

associated with online loan applications, Online Fraud (30%), encompassing activities such as shopping fraud, investment scams, job recruitment fraud, and romance scams, Online Blackmail (12%), Unauthorised Access (9%), and Online Impersonation (4%). The cumulative monetary losses as of June 2023 amounted to 49.5 million Ghana Cedis.

Mr. Oppong commended the NSB for organising the awareness session for its staff and stakeholders and added that as a member of the JCC, such an initiative was apt and demonstrated the Bureau's commitment to help secure a safer and resilient digital cyberspace for all.

He revealed that the CSA had begun the licensing and accreditation of CSPs, CEs and CPs as mandated by the Cybersecurity Act 2020 (Act 1038) and solicited support from the NSB to enforce cybersecurity laws and regulations in Ghana.

## Remarks and Launch

### **Kwabena Adu-Boahene**

Director-General of the National Signals Bureau (NSB)

In his submission, Mr. Kwabena Adu-Boahene delved into pertinent issues and essential components

**Kwabena Adu-Boahene**

Director-General of the National Signals Bureau (NSB)

related to the National Cyber Security Awareness Month. He expressed apprehension regarding the escalating incidents of insider threats within the cybersecurity landscape and the susceptibility of humans as the weakest links in the chain of cyber defences. He cited notable security breaches in institutions, including banks, underscoring the critical role humans play in cybersecurity vulnerabilities.

Mr. Adu-Boahene indicated that issues of misinformation and disinformation are a major concern deserving urgent attention, especially in the upcoming electoral year. He further underscored the urgency of addressing the associated implications of misinformation and disinformation and called for collaborative efforts to establish robust protocols for combatting the dissemination of false information. He officially launched the Cyber Security Awareness Month for the National Signals Bureau.

## Conclusion

In conclusion, Ms. Debrah Tetteh and Mr. Abdul Hamid, both representing the National Signals Bureau, expressed gratitude and appreciation as they delivered the vote of thanks and closing prayer, respectively, concluding the NSB event launch.

# CYBERSECURITY AWARENESS SESSION FOR STAFF OF THE GHANA PRISONS SERVICE

## Background

The Cyber Security Authority (CSA) as part of its awareness creation activities during the National Cyber Security Awareness Month (NCSAM) facilitated an awareness session for the staff of the Ghana Prison Service (GPS) to increase their cybersecurity consciousness to promote the digitalisation agenda of the country. The hybrid session was held to educate staff of the GPS on cybersecurity trends, threats, and preventive measures.

In attendance were Major General A. Y. Nsiah, a member of the Joint Cybersecurity Committee (JCC) of the CSA, Mr. Alexander Oppong, a management member of the CSA (representing the Director General of CSA), selected staff of the Cyber Security Authority, senior and junior officers of the Ghana Prisons Service across the country.



**Benedict Bob-Dery**  
Director of Human Resource, Ghana Prisons Service

technologies. He urged participants to take the session seriously and to acquire sufficient information to safeguard themselves in the ever-evolving digital landscape.

## Remarks

**Benedict Bob-Dery**

Director of Human Resource, Ghana Prisons Service

Mr. Bob-Dery expressed his appreciation to the Director-General and team of the CSA for facilitating the session. He indicated that the theme for this year's NCSAM "Promoting a Culture of Digital Safety" was truly relevant in the era of digitalisation and its associated increased rate of cybercrime.

The Director noted that digitalisation is gradually taking over all aspects of life, including financial services, e-commerce, and tax payments. He emphasised the alarming surge in cybercrime causing pecuniary loss of millions of Ghana cedis to individuals and entities, attributing it to criminals exploiting the widespread adoption of digital

## Presentation

**Isaac Socrates Mensah**

Cyber Security Authority

Mr Mensah of the Computer Emergency Response Team (CERT) of the CSA gave an extensive presentation on cybersecurity developments in the cyber world, noting that about one hundred percent security of every user of the internet is vulnerable to cyber-attacks.

Mr. Mensah highlighted some global and domestic cyber trends including the Australian prison attack, the US pipeline incident where the volume of chlorine used to filter water was increased by cyber criminals, and the loss of Gambia's Central bank's financial data to criminals causing a state of national emergency. He stated that romance fraud, associated





**Isaac Socrates Mensah**  
Cyber Security Authority

cyberbullying, shopping fraud, online blackmail, and unauthorised access are some common cybersecurity incidents which the officer must be careful of.

He indicated further that malware, malicious apps, shoulder surfing and theft are some threats

with the use of mobile devices. Some security measures he mentioned could be used to protect against these attacks are encryption, multi-factor authorisation, regular update of systems, installation of security software and constant review of app permissions.

He advised participants to be cautious of the content they share on social media, stay up to date on security issues as the landscape keeps changing frequently and to also follow the CSA on its social media handles for frequent updates.

## Conclusion

Participants expressed appreciation for the in-depth delivery by the CSA official and expressed commitment to staying safe online and also to educating others on the need for cyber hygiene practices.



# CYBERCRIME AND CYBERSECURITY SENSITISATION ENGAGEMENT AT THE ECONOMIC & ORGANISED CRIME OFFICE

## Background

The Economic and Organised Crime Office (EOCO) as part of the activities marking the 2023 National Cyber Security Awareness Month (NCSAM) organised a hybrid cybersecurity sensitisation for their personnel. The sensitisation event was targeted at enhancing the knowledge and skills of the personnel to protect themselves online, adopt responsible digital behaviour, and respond effectively to potential threats.

### Remark

**S.O. Sedina Gbeve**  
EOCO staff

S.O. Sedina Gbeve, an official of EOCO, noted the importance of cybercrime issues and acknowledged the Cyber Security Authority (CSA) for organising the National Cyber Security Awareness Month and making the workshop possible. She referenced a report by the National Computer Emergency Response Team, which noted that, 49.5 million Ghana Cedis was lost to cybercrime from January to June of 2023 and indicated the need for officers of EOCO to gain knowledge to better equip themselves against cyber threats through workshops like this.

The Director of Administration of EOCO, P.S.O Edward Cudjoe, said cybersecurity is a part of the Office's internal trainings, and therefore it was necessary that the staff use the opportunity granted by the workshop to refresh their memories on current issues on cybercrime and emerging trends.

### Remarks

**Alexander Oppong**  
Acting Director of Capacity Building and Awareness Creation

The Ag. Director of Capacity Building and Awareness Creation, (CBAC), Mr. Alex Oppong, speaking on behalf of the Director-General of the Cyber Security Authority, Dr. Albert Antwi-Boasiako gave some

insights on the incidents reported to the National Computer Emergency Response Team (CERT) of the CSA through the cybersecurity/cybercrime incident reporting Points of Contact (POCs (points of contact)) by the citizenry stating that from January to September 2023. Of a total of nine thousand two hundred and ninety-six (9,296), major crimes reported on included online loan applications, online fraud which includes shopping fraud, investment frauds, job recruitment fraud, romance fraud among others, online blackmail, unauthorised access, and online impersonation.

Mr. Oppong emphasised the need for continuous collaborations among intelligence institutions managing cybercrime/cybersecurity incident reporting channels to collate the statistics and generate a comprehensive national report to enable drive national policies and strategies on cybercrime and cybersecurity.

## Presentation

Presenting on Cyber Crime and Cyber Security, the Head of Public Affairs for the Economic and Organised Crime Office (EOCO), S.O. Faustina Lartey, threw light on the types of cybercrime, what cybersecurity is, and how participants can secure their mobile devices, surf social media safely and best practices for cybersecurity.

## Conclusion

Following an interactive session after the presentation, the Deputy Executive Director, Operations of EOCO, Mr. Bashiru Dapilah, indicated that it is necessary to continue to learn about new threats and best practices in the cyber landscape due to the ever changing nature of the threats, in order to be well equipped. He further encouraged the participants to share their acquired knowledge with family and friends.

# PROMOTING CYBERSECURITY CONSCIOUSNESS AMONG THE STAFF OF THE RESEARCH DEPARTMENT

## Background

The CSA as part of collaboration with members of the Joint Cybersecurity Committee (JCC), organised cybersecurity sensitisation event for the staff of the Research Department as part of the National Cybersecurity Awareness Month (NCSAM).

In attendance were the Director-General of the Research Department, Mr. Peter Opata, the Director-General of the Cyber Security Authority, Dr. Albert Antwi-Boasiako, Directors of the Research Department, staff of the Cyber Security Authority, and staff of the Research Department.

### Remarks

**Peter Opata**

Director-General, Research Department

Mr. Peter Opata, in his address, expressed his gratitude to the Director-General of the CSA, Dr. Albert Antwi-Boasiako for his role in making the workshop a reality.

He mentioned the risks associated with the use of smart devices and commended Dr. Antwi-Boasiako for annually facilitating the National Cybersecurity Awareness Month. He added that the initiative serves as a vital component in raising awareness about cybersecurity and its importance.

Mr. Peter Opata acknowledged the significance of stakeholder engagements and the learning opportunities they offer as urged participants to remain abreast of emerging trends in the ever-evolving cyber landscape.

### Remarks

**Dr. Albert Antwi-Boasiako**

Director-General of the CSA

Dr. Albert Antwi-Boasiako expressed his appreciation for the support rendered by the Research Department, a key ally on both the Joint Intelligence Committee and the Joint Cybersecurity Committee.

He highlighted the advancements Ghana has made in cybersecurity development, noting that Ghana has been ranked 3rd in Africa and 43rd globally in terms of cybersecurity readiness. He emphasised that this achievement has been facilitated through collaborative efforts involving institutions such as the Research Department.

Responses from participants underscored the importance of globalisation and the increasing dependence on digitalisation, creating a pressing need for such sensitisation efforts.

Dr. Albert Antwi-Boasiako urged the participants to exercise caution when sharing information on social media.

### Presentation

**Gerald Awadzi**

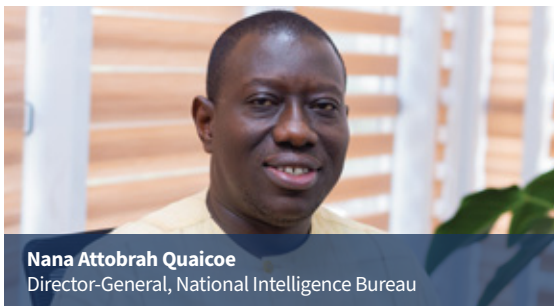
Cyber Security Authority

The facilitator, Mr. Gerald Awadzi's presentation focused on the types of cyber threats such as malware, phishing, social engineering, cyber best practices. He advised the general public to ensure regular updates of applications and to install anti-virus software to protect their devices. During the question-and-answer session, participants raised several questions related to online security.

# CYBERSECURITY WORKSHOP FOR DIRECTORS OF THE NATIONAL INTELLIGENCE BUREAU (NIB)

## Background

The CSA in collaboration with members of the Joint Intelligence Committee (JIC) held a virtual cybercrime and cybersecurity sensitisation workshop for executive members of the NIB to enhance the knowledge and skills of the Bureau. The purpose was to ensure they protect themselves online, adopt responsible digital behaviour, and respond effectively to potential threats. In attendance were Dr. Albert Antwi-Boasiako; Director-General, CSA, Nana Attobrah Quaicoe; Director-General, National Intelligence Bureau, Executive Director; Economic and Organised Crime Office (EOCO), COP Maame Yaa Tiwaa Addo-Danquah, Directors of the National Intelligence Bureau, and Mr. Alexander Oppong; Ag. Director, Capacity Building and Awareness Creation, CSA.



**Nana Attobrah Quaicoe**  
Director-General, National Intelligence Bureau

## Remarks

**Nana Attobrah Quaicoe**

Director-General, National Intelligence Bureau

Nana Attobrah Quaicoe in his remarks stated that technology has become the biggest enabler for individual and organisational efficiencies, noting that without technology it would be difficult to identify and detect threats and vulnerabilities and their impact on business continuity. He therefore recommended threat modelling and cybersecurity awareness be part of the organisational culture of the NIB.

## Remarks

**Dr. Albert Antwi-Boasiako**

Director-General of the CSA

Dr. Antwi-Boasiako noted the importance of personal and organisational information security and encouraged the NIB to validate the authenticity of information before sharing with third parties. He additionally tasked the personnel of the Bureau to practice personal information security by enforcing cyber hygiene practices and avoiding the use of open public WIFI, among others. He further urged the NIB to extend cybersecurity education to their families at home and abroad and adding that the CSA and the E-Crime Bureau would collaborate with the NIB to enhance their digital forensics skills and experience.

## Presentation

**Isaac Socrates Mensah**

Cyber Security Authority

Mr Socrates Mensah's presentation highlighted the statistics and trends of global digital mobile device usage, Ghana's position on the global scale and the trends of cyber incidents based on data available to the CSA. He concluded by encouraging participants to stay vigilant when online and to report suspicious online activities to the National Computer Emergency Response Team incident reporting points of contact of the CSA.

Mr Alexander Oppong of the CSA gave the closing remarks and indicated the importance of developing a safer digital culture and the need for all to be mindful of cybersecurity risks when online.



# CYBERCRIME AND CYBERSECURITY SENSITISATION ENGAGEMENT - NARCOTICS CONTROL COMMISSION (NACOC)

## Background

The CSA partnered the Narcotics Control Commission (NACOC), a member institution of the Joint Intelligence Committee (JIC) to organise a cybersecurity sensitisation workshop aimed at advancing and imparting knowledge about cybersecurity best practices to the staff of the Narcotics Control Commission.



## Welcome Address

**Kenneth Adu-Amanfoh**

Director-General of the Narcotics Control Commission

Mr. Kenneth Adu-Amanfoh in his address commended the notable growth of cybersecurity in Ghana, stressing the significant paradigm shift in criminal activities from conventional physical tools and equipment to the use of the internet and associated digital tools.

He acknowledged the involvement of both the Narcotics Control Commission and the Cyber

Security Authority in the Joint Intelligence Committee, highlighting the importance of addressing cyber threats across all strata of society. Mr. Adu-Amanfoh further elaborated on the proactive steps taken by the Cyber Security Authority to combat cybercrime, emphasising the gravity of cybercrime, and urged officers from across the country to actively engage and participate in addressing the menace.

Concluding his remarks, Mr. Adu-Amanfoh urged officers to actively promote cybersecurity awareness to develop cyber resilience.

## Presentation

**Gerald Awadzi and Mr. Joseph Attoh**

Cyber Security Authority

The presentations focused on the various aspects of cybersecurity, distinct types of cyber threats, and insights into concepts such as malware, phishing, social engineering, cyber best practices, mobile device security and practical sessions on email account compromise.

Mr. Awadzi and Mr. Attoh advised participants to regularly check if their email accounts have been compromised, in a bid to empower them with a proactive approach to safeguard their online information.

The Acting Director of Capacity Building and Awareness Creation, Mr. Alex Oppong, in his remarks commended the management of the NACOC for their partnership and highlighted the rationale of the collaboration.

# CYBERSECURITY SENSITISATION FOR EXECUTIVE MEMBERS OF THE CUSTOMS DIVISION OF THE GHANA REVENUE AUTHORITY

## Background

To promote a culture of digital safety, the CSA leveraged the 2023 edition of the NCSAM to organise cybercrime and cybersecurity sensitisation engagements with the Customs Division of the Ghana Revenue Authority (GRA). The sensitisation engagement was to ensure a heightened awareness of cybercrime and cybersecurity issues among the staff of the Customs Division with the aim of preventing and mitigating of cybersecurity incidents.

### Remarks

**Alexander Oppong**

Acting Director of Capacity Building and Awareness Creation

Mr. Alexander Oppong, the Acting Director, Capacity Building and Awareness Creation at the CSA delivered remarks on behalf of the Director-General of the CSA. He noted the significance of NCSAM in fostering a collective mindset to promote a culture of digital safety.

Highlighting the potential threat to critical systems in organisations due to the availability of critical data, Mr. Oppong underscored the need for vigilance, noting prevalent cyber-attacks in the cyberspace including business email compromise, cyber fraud, and phishing.

He urged participants to stay updated about cyber threats and to adopt a proactive approach, in mitigating risks and enhancing the overall cybersecurity posture of the organisation.

### Presentation

**Joseph Antwi-Attoh**

Cyber Security Authority Official

In his presentation, Mr. Joseph Antwi-Attoh, shared insights on global digital mobile device usage trends, Highlighting that Ghana was the 8th highest user of social media and the 21st in social media usage for work globally.

Mr. Antwi-Attoh identified Cyberbullying, Online fraud, and Online blackmail as the top three reported cyber incidents at the national CERT. He provided valuable insights to participants, urging them to use strong passwords, avoid free and pirated software, and emphasised the significance of cyber awareness in preventing cyberattacks.

### Remarks

**ACP Rosemary Addo Parker**

Head of Customs Technical Service Bureau

ACP Rosemary Addo Parker expressed her gratitude to the Cyber Security Authority for organising the event to educate the Ghana Customs Service on cyber security awareness. She acknowledged the importance of building a culture of digital safety and commended the CSA for its efforts in this regard.

She urged the participants to share the knowledge gained during the event and emphasised the importance of practising confidentiality in handling information. This, she said, underscored the commitment to maintaining the security and integrity of data within the Ghana Customs Service.



## WORKSHOP ON CYBERSECURITY SENSITISATION FOR EXECUTIVE MEMBERS AND STAFF OF THE GHANA NATIONAL FIRE SERVICE HEADQUARTERS, ACCRA

### Background

The CSA joined the Ghana National Fire Service (GNFS), a member of the Joint Intelligence Committee to create cybersecurity awareness among the staff of the GNFS. The goal of the workshop was to ensure that staff are well equipped to protect themselves online, adopt responsible digital behaviour, and respond effectively to potential threats.

### Remarks

**Julius Kunor**

Chief Fire Officer (CFO), Ghana National Fire Service

CFO Kunor commenced his remarks by expressing profound gratitude to the Director-General of the CSA, Dr. Albert Antwi-Boasiako, for organising the



**Julius Kunor**  
Chief Fire Officer (CFO), Ghana National Fire Service

workshop. He proceeded by emphasising the critical nature of the cyberspace and underscored the necessity for increased attention and vigilance in that domain. He reiterated the primary objectives of the workshop, underscoring its purpose of imparting knowledge and fostering a culture of digital safety.

CFO Kunor urged the officers to actively participate in the workshop to acquire valuable insights, and develop skills in cybersecurity.



## Presentation

**Stephen Cudjoe-Seshie**  
Lead, National CERT, CSA

Mr. Stephen Cudjoe-Seshie, spoke on behalf of the Director-General, Dr. Albert Antwi-Boasiako, and highlighted the critical importance of information security for both individuals and organisations within government institutions to protect national digital assets.

Mr. Cudjoe-Seshie stressed the necessity of ongoing collaboration between the CSA and government institutions to bolster cyber capabilities and resilience, which are essential drivers of Ghana's digital transformation.



**Joseph Antwi-Attoh**  
Cyber Security Authority

## Presentation

**Joseph Antwi-Attoh**  
Cyber Security Authority

Mr. Joseph Antwi-Attoh's presentation provided statistics on global digital mobile device usage trends and Ghana's emergence as a significant player, ranking 8th worldwide in social media usage and 21st in using social media for professional purposes.

A significant aspect of the presentation focused on the 2019 and 2022 cybersecurity incidents data recorded by the CSA, with the top three reported cyber incidents to the National Computer Emergency Response Team (CERT) of the CSA, being cyberbullying, online fraud and blackmail and its implications on cybersecurity. He further provided crucial cybersecurity tips to the participants, as he stressed the importance of using strong passwords and avoiding the use of free and pirated software.

## Conclusion

The event concluded with a call to action, urging participants to implement controls for online security.



# WORKSHOP ON THE COST OF DATA BREACH FOR STAKEHOLDERS OF NITA

## Background

The National Information Technology Agency (NITA), a Joint Cybersecurity Committee (JCC) member, organised a workshop aimed at creating awareness on the cost of data breach and the ways to safeguard data.



**Richard Okyere-Fosu**  
Director-General, National Information Technology Agency (NITA)

## Welcome Remarks

**Richard Okyere-Fosu**  
Director-General National Information Technology Agency (NITA)

Mr. Richard Okyere-Fosu stated that workshops of this nature are necessary to sharpen the skills of participants in the field of information technology which is characterised by constant change. He noted that cybersecurity is the other side of the coin in an era of digitalisation and hence, cyber hygiene practices must be at the fingertips of everyone who uses computer technologies and more especially for staff of NITA and their stakeholders.



**Dr. Albert Antwi-Boasiako**  
Director-General, Cyber Security Authority

## Presentation Summary

**Dr. Albert Antwi-Boasiako**  
Director-General, Cyber Security Authority

Dr. Albert Antwi-Boasiako in his remarks stated the importance of establishing robust data management systems as government institutions. He noted that a section of public sector institutions have been identified as Critical Information Infrastructure and stressed on the need to employ the right technologies to protect such data systems. He also highlighted the direct costs associated with cyber incidents, citing a specific case in Ghana where a company incurred over GH¢100 million in direct financial losses.

He concluded his remarks by noting the measurable progress that government institutions can make in securing the digital economy and expressed the CSA's commitment to fully support NITA and its stakeholders.

## Presentation

Facilitators from Oracle Ghana educated participants on data management, data security, and data analysis solutions that Oracle provides. They emphasised the importance of government sector institutions to secure data by adopting and using modern data management systems.

## Conclusion

Mr Richard Okyere-Fosu, the Director-General of NITA, in bringing the event to an end emphasised that cybersecurity requires a collaborative effort, and it is incumbent upon participants to strive for a secure digital ecosystem.



Facilitators from Oracle Ghana delivering their presentation



A group picture of participants from the workshop

# 04.

**High Level Capacity Building  
and Awareness Creation Events**



# CONSULTATIVE WORKSHOP ON THE DEVELOPMENT OF THE ACCREDITATION FRAMEWORK TO ACCREDIT SECTORAL COMPUTER EMERGENCY RESPONSE TEAMS

## Opening Remarks

**Mercy Araba Kertson**

Acting Director of Administration,  
Cyber Security Authority

Madam Mercy Araba Kertson, the Acting Head of Administration at the Cyber Security Authority (CSA), delivered a speech on behalf of the Director-General, Dr. Albert Antwi-Boasiako, highlighting the borderless nature of the digital world, and emphasising its numerous advantages and potential threats.

Madam Kertson highlighted Section 44 of the Cybersecurity Act, 2020 (Act 1038), which mandates the CSA to establish sectoral CERTs and oversee their operations. She stressed the importance of the accreditation process to integrate and streamline sectoral CERTs within the national CERT ecosystem. This process, she noted, would strengthen relationships, ensure conscious reporting, and tracking of incidents, and facilitate the sharing of information and procedures in accordance with international best practices.

Focusing on the National Cyber Security Awareness Month (NCSAM) 2023, Madam Kertson highlighted its significance as an opportunity to engage with stakeholders responsible for hosting Ghana's sectoral CERTs. She announced plans to finalise the mapping of constituents to each sector, to gather updates on the development of the accreditation framework through meetings with relevant representatives and stakeholders within the CERT ecosystem. This initiative aims to align with key stakeholders and enhance collaboration to effectively address cybersecurity challenges.

## Presentation

**Stephen Cudjoe-Seshie**

Lead, National CERT, CSA

Mr. Stephen Cudjoe-Seshie presented a diagram illustrating the establishment of nine sectoral CERTs, each with a dedicated lead institution. These sectors included government, telecommunications, banking and finance, national security, academic, transport, military, energy, utility, and health.

He explained, that there are some already established sectoral CERTs; NITA for the government, NCA for telecommunications, and the Bank of Ghana for banking and finance. He added that the military and the other sectors are yet to establish their CERTs."

Mr. Cudjoe-Seshie outlined the vision of establishing sectoral Computer Emergency Response Teams (CERTs) operating an information-sharing infrastructure. This infrastructure, he said aims to facilitate easy access to information between the sectoral CERTs, highlighting the ongoing process of forming and accrediting the sectoral CERTs to achieve this collaborative vision.

## Conclusion

The session was interactive as participants shared ideas and sought clarification on the establishment of their sectoral CERTs. The participants collectively resolved to share intelligence and follow up on issues through the Authority's official contacts.



## SECTOR CERTs UPDATE WORKSHOP

### Background

The event was expected to provide an opportunity to evaluate the maturity of existing Sectoral Computer Emergency Response Teams (CERTs) and encourage the sharing of information and best practices, particularly in light of ongoing efforts to operationalise the Energy Sector CERT.

A workshop was thus held on October 25, 2023, at Ghana India Kofi Annan Centre of Excellence in ICT as part of NCSAM 2023 activities.



**Dr. Albert Antwi-Boasiako**  
Director-General, Cyber Security Authority

### Opening Remarks

**Dr. Albert Antwi-Boasiako**  
Director-General, Cyber Security Authority

The Director-General of the CSA, Dr. Albert Antwi-Boasiako highlighted the key role of CERTs in incident response and how the effective implementation of Ghana's sectoral CERT ecosystem will support a secure and resilient digital ecosystem, emphasising the need for information sharing and collaboration.



**Kobina Richardson**  
Director, Information Security Office of the Bank of Ghana (BoG)

### Presentation Summary

Mr. Kobina Richardson, Director, Information Security Office of the Bank of Ghana (BoG) represented the Deputy Governor of the Bank. He presented the impact of the 2018 Cyber and Information Security Directive for financial institutions to be licensed, registered, or regulated by the Bank of Ghana and how it has improved cyber resilience in the financial sector. He pledged the commitment of the BoG to continue to deepen collaboration with the CSA in ensuring that the sector and the overall digital ecosystem of Ghana are secure and resilient.

The Director-General of the National Communications Authority (NCA) represented by Madam Olivia Okailey Quartey, the Deputy Director-General for Managerial Operations, commended the CSA's efforts in the development of the cybersecurity sector and suggested closer collaboration with sector agencies via mechanisms such as the Joint Cybersecurity Committee to drive initiatives in the ecosystem.



**Olivia Okailey Quartey**  
Deputy Director-General for Managerial Operations, NCA



**Nii Ankrah**  
Information Security Officer, BOG



**Hon. William Owuraku Aidoo**  
Deputy Minister for Energy



**John Bambio**  
Technical Focal Person, Energy Sector CERT Project Team

Hon. William Owuraku Aidoo, Deputy Minister for Energy indicated the Ministry's commitment to comply with Section 44 of the Act 1038 adding that a project implementation committee has commenced work to set up the Energy sector CERT.

Mr. Nii Ankrah, Information Security Officer, BOG and Mr. John Bambio, Technical Focal Person at the Energy Sector CERT Project Team delivered presentations highlighting the core services their respective institutions offer to constituents mapped onto the Forum for Incident Response and Security

Teams (FIRST) Services framework, operations, and funding models. The BoG presentation gave an overview of major threats discovered and reported within the sector such as credential theft, and unpatched legacy systems with Internet exposure.

## Recommendation

Collaboration is the foundation for an effective CERT ecosystem, therefore ongoing engagements led by the National CERT situated at the CSA are very apt.

# WORKSHOP ON CRITICAL INFORMATION INFRASTRUCTURE (CII) SECURITY AND RISK MANAGEMENT

## Background

As part of the measures to effectively promote a culture of digital safety and hygiene, the Cyber Security Authority (CSA) leveraged on the 2023 edition of the National Cybersecurity Awareness Month to provide a forum to engage with Critical Information Infrastructure(CII) owners on utilizing cybersecurity risk management concepts, standards, and frameworks as an operational tool to mitigate or minimize the impacts of cyber risks on CII's.



**Mercy Araba Kertson**  
Ag. Director of Administration

## Opening Remarks

**Mercy Araba Kertson**  
Ag. Director of Administration

Madam Mercy Araba Kertson, the Ag. Director, Administration delivered the remarks on behalf of the Director-General, CSA. Noting the significance of NCSAM, Madam Mercy Kertson stressed the need for

technical leaders who steer the course of the nation's CII to safeguard these critical systems. She revealed the harrowing amounts lost by individuals to cybercrime as recorded by the National Computer Emergency Response Team of the Cyber Security Authority in the first six months of 2023.

Madam Mercy Araba Kertson added that CII Security and Risk Management is not merely a technical challenge but a societal imperative and requires a governmental and societal approach to ensure a safer digital future.



**Roger Akrong**  
Chief Information Security Officer, ECG

## Presentation

**Roger Akrong**  
Chief Information Security Officer, Electricity Company of Ghana

Mr. Roger Akrong made a presentation on the topic, "Securing CII's: Effective Risk Management Strategies". His presentation explained the various provisions in the Cybersecurity Act, 2020, (Act 1038) related to Critical Information Infrastructure owners

as specified in, sections 35-40 and 92 of the Act. He further highlighted prevalent cybersecurity threats affecting CIIs worldwide, such as ransomware attacks, malware attacks, and phishing attacks and encouraged PoCs to implement multiple risk assessment controls. He additionally took the participants through the concepts of risk management framework, and the qualitative and quantitative risk assessment and encouraged risk communication among participants and their management.

## Recommendations and Conclusion

The following recommendations were made at the end of the event;

- CII owners should leverage blockchain techniques to ensure data integrity in cyber risk management.
- CSA should develop and enforce a risk assessment and management framework for CII owners.
- Case studies on risk assessment and management should be made available to serve as reference.

Madam Adjoa Asamoah Tabi-Asiamah, an official of the CSA, in conclusion, echoed that the CSA will involve CII owners in respective CII registration validation engagements, and urged participants to practicalize the knowledge gained at the workshop.

# WORKSHOP ON THE ROLE AND IMPACT OF CYBERSECURITY GOVERNANCE IN THE PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE (CII)

## Background

The purpose of the workshop was to create a platform for meaningful engagement with the Critical Information Infrastructure (CII) owners. The event which was themed the “Role and Impact of Cybersecurity Governance in the Protection of Critical Information Infrastructure (CII)”, highlighted the role of CII Owners in CII protection, emphasising compliance with CII regulations and directives, and fostering a culture of information sharing to enhance digital safety.

## Opening Remarks

**Adelaide Benneh Prempeh**

Board Member, CSA

Delivering the remarks on behalf of the Director-General of CSA, Mrs. Adelaide Benneh Prempeh commended the CII owners for their participation in registering their critical information infrastructure in accordance with Section 36 of the Cybersecurity Act, 2020 (Act 1038).

Mrs. Adelaide Benneh Prempeh emphasised the importance of implementing robust and legal measures to ensure the protection of CIIs.



Additionally, she pointed out that supply chains are a prime target for malicious actors, citing incidents such as the SolarWinds attacks and the COVID-19 hack. She reassured participants that efforts are underway to mitigate cyber threats.



**Carl Sackey**  
Board Member, CSA

## Presentation

**Carl Sackey**  
Board Member, CSA

Mr. Carl presented on "Cybersecurity Governance Structures within an organisation". He highlighted the increasing reliance of institutions on digital technologies for their operations and underscored the pivotal role of the Board of any organisation in ensuring judicious investments in appropriate cybersecurity technologies.

He noted the imperative need for every Critical Information Infrastructure (CII) organisation to appoint a Chief Information Security Officer (CISO), adding that cybersecurity should be viewed as a strategic investment, that when executed correctly, can positively influence overall organizational functionality.

In conclusion, Mr. Carl Sackey urged organisations to establish a cybersecurity framework and roadmap.



**Adelaide Benneh Prempeh**  
Board Member, CSA

## Presentation

**Adelaide Benneh Prempeh**  
Board Member, CSA

Mrs. Adelaide Benneh-Prempeh delivered a presentation on the "Legal Implications for Cyber Governance". Her presentation highlighted key elements and implications, with a specific focus on cyber governance. She underscored that legislation as specified in section 97 of the Cybersecurity Act 2020, (Act 1038) provides the CSA with the foundation for identifying owners of Critical Information Infrastructure (CII) and designating CII institutions.

She highlighted that the policies addressing risks align with international best practices and advised participants to have a cybersecurity expert on their management boards. Furthermore, she recommended that CII owners integrate cybersecurity measures into their technical and organisational frameworks.

## Presentation

**Kobina Nkum Akwa**  
Financial Technologist, Mango InfoSec Solutions

Mr. Kobina Nkum Akwa delivered a presentation on "Cybersecurity Strategy Formation" tailored for



organizations. Relevant statistics in his presentation analysed the costs associated with cyber breaches, emphasising the urgency of addressing cybersecurity issues. Mr. Akwa advised the audience to actively involve Board members and management in cybersecurity governance events and activities.

## Conclusion

The workshop successfully fostered a constructive dialogue among Critical Information Infrastructure (CII) owners, emphasizing the pivotal role of cybersecurity governance in protecting CII and providing valuable insights and recommendations for enhancing digital safety and resilience within organisations.

## PANEL DISCUSSION ON ‘SAFEGUARDING ELECTORAL INTEGRITY, PEACE AND SECURITY, PRACTICAL POLICIES AND STRATEGIES TO COMBAT DISINFORMATION’



### Welcome Remarks

**Hon. Kojo Oppong Nkrumah**  
Minister for Information

Hon. Kojo Oppong Nkrumah commenced his remarks by extending a warm welcome to all the present. He highlighted the prevalence of disinformation during the February 2023 elections in Nigeria, where several websites were created to disseminate fake information for political propaganda.

Hon. Oppong Nkrumah further mentioned that during the COVID-19 era, around one-third of media practitioners disseminated unverified information online, indicating the challenge of misinformation even among professionals.

In his conclusion, Hon. Oppong Nkrumah noted the possibility of misinformation and disinformation being used by political actors in the lead-up to Ghana's 2024 elections and called for strategies to counteract misinformation and disinformation during this crucial period.



**Kelvin Casas-Zamora**  
Secretary-General, International IDEA

## Keynote Address

**Kelvin Casas-Zamora**

Secretary-General, International IDEA

Mr. Kelvin Casas-Zamora revealed how critical it is for Ghana to combat the worldwide problem of disinformation and misinformation and how the International IDEA is attempting to address it by creating a new workstream that examines the relationship between democracy and digitalisation.

He noted that the organisation is working on projects to safeguard election integrity by offering technical assistance, advising election management bodies on best practices, and developing projects to help election authorities use digital spaces for stakeholder outreach, strategic communications, and civic education initiatives.

He suggested that it is vital to build up public defences against a potentially harmful information environment, adding that new rules for using social media and digital media in Ghana's elections will be released by the Association of African Electoral Authorities.

In conclusion, Mr. Casas-Zamora stated that to strengthen democracy in the digital age, civil society and other partners should work to increase civic awareness and democratic literacy to counter the weight of disinformation. Likewise, social media companies should reflect on the role their recommender systems play in guiding people towards defamatory content.

## Panel Discussion

The First Panel Discussion on “Disinformation, Electoral Integrity and National Security” convened esteemed speakers, including Mr. Kwaku Krobea Asante, Dr. Serebour Quaicoe, and Professor Vladimir Antwi-Danso, moderated by Mamavi Owusu-Aboagye.

The panelists collectively emphasised the importance of transparency, professional integrity, and security in Ghana's electoral processes. Their insights underscored the need for proactive measures to safeguard democracy and combat the dissemination of false information, urging stakeholders to fulfil their roles effectively for the upcoming elections.

In another development, a panel discussion, moderated by Hon. Fatimatu Abubakar, delved into the multifaceted challenge of “Safeguarding electoral integrity, peace and security, practical policies and strategies to combat disinformation”. Dr. Yaw Boadu highlighted the distinction between misinformation and disinformation, stressing the importance of verifying political information before dissemination. Madam Kathleen Addy emphasised the critical role of civic education in shaping public opinion and outlined strategies employed by the National Commission for Civic Education (NCCE) to counter misinformation, underscoring its importance for national development.

Dr. Albert Antwi-Boasiako, Director-General of the Cyber Security Authority, highlighted collaborative efforts with electoral bodies and networks to enhance internal risk management processes and advocated for educational initiatives to deter individuals from engaging in disseminating false information. Additionally, Mr. Frank Oye emphasised the importance of technological solutions and legal frameworks in combating disinformation and ensuring electoral integrity.

## Conclusion

H.E. Mrs. Sylvia Naa Adaawa Annoh, Ghana's ambassador to Denmark and Sweden, concluded the event with the closing statement and Madam Dzifa Bampoe, the moderator expressed gratitude to all participants and dignitaries who attended the program.

# INTRODUCTORY COURSE ON CYBERCRIME AND ELECTRONIC EVIDENCE FOR JUDGES IN GHANA

## Background

The Cyber Security Authority (CSA), in collaboration with the Technical Assistance and Information Exchange Instrument (TAIEX) and with support from the Council of Europe, organised a 3-day workshop to support cyber-capacity building to promote the Budapest Convention on Cybercrime and improve prosecutors' skills in electronic evidence handling.



**Massimo Mina**  
Head of Cooperation, Delegation of the European Union to Ghana/TAIEX Instrument

## Opening Remarks

**Massimo Mina**

Head of Cooperation, Delegation of the European Union to Ghana/TAIEX Instrument

Mr. Massimo Mina indicated that personnel of the judicial services must be equipped with the necessary knowledge and tools to effectively combat cybercriminals. Mr. Mina highlighted that the workshop will provide participants with a comprehensive understanding of cybercriminals'

operations to aid in investigating and prosecuting cybercrime cases to ensure that justice is fair, and the perpetrators are held liable. He emphasised that judges and prosecutors also need to explore international best practices and legal frameworks that cover cybercrime and cybersecurity.

## Remarks

**Cosmina Menghes**

Programme Officer, Council of Europe (CoE)

In a remark delivered on behalf of Ms. Catalina Stroe, Project Manager, GLACY+ Project, Ms. Cosmina Menghes, elaborated that cybercrime is a global crime that needs international cooperation, stating that business email compromise (BEC), phishing, online child sexual exploitation and abuse (OCSEA), and cyberbullying, among others, compromise the security of online experiences. She further indicated that the Budapest Convention, which serves as a reference to cybercrime in general, has been rectified by 16 countries worldwide. Ms. Menghes further outlined the CoE's support for Ghana's commitment to fighting cybercrime and encouraged all to fully participate in the 3-day workshop.

## Remarks

**Dr. Albert Antwi-Boasiako**

Director-General, Cyber Security Authority

The Director-General of the CSA, Dr. Albert Antwi-Boasiako, acknowledged the Chief Justice for her commitment towards digital transformation. He indicated that the workshop aimed at tackling the increasing cybercrime threats in Ghana and Africa by sharing knowledge on the detection, investigation, and prosecution of cybercrimes. He further stated that the Cloud Evidence Group proposes measures





**Dr. Albert Antwi-Boasiako**  
Director-General, Cyber Security Authority

to enable fast and effective access to electronic evidence while respecting human rights and the rule of law. Dr. Albert Antwi-Boasiako added that Capacity building is an effective way to address cybercrime and challenges related to electronic evidence noting that the implementation of the Budapest Convention on Cybercrime, will improve prosecutors' and judges' skills, and adjudicate cases of cybercrime involving electronic evidence.

## Remarks

### Jacob Soung

Deputy Director, Judicial Training Institute

Mr. Jacob Soung, Deputy Director of the Judicial Training Institute (JTI), representing the Director of the JTI, Justice Issifu Omoro Tanko Amadu highlighted the transformative impact of information technology (IT) on contemporary life, noting its pervasive presence in daily activities. While IT has significantly improved lives and facilitated access to rights, Mr. Soung underscored the associated risks, particularly in Ghana's context, where cybercrimes such as internet fraud and identity theft pose continuous threats.

He however emphasised Ghana's proactive measures in promoting cybersecurity through



**Jacob Soung**  
Deputy Director, Judicial Training Institute

legislative frameworks such as the Electronic Transactions Act, of 2008, the Cybersecurity Act, 2020 (Act 1038), and the Data Protection Act, 2012, aimed at addressing cybercrimes and enhancing cybersecurity. He urged participants to actively engage in the forthcoming discussions to generate meaningful solutions for addressing socio-legal issues.

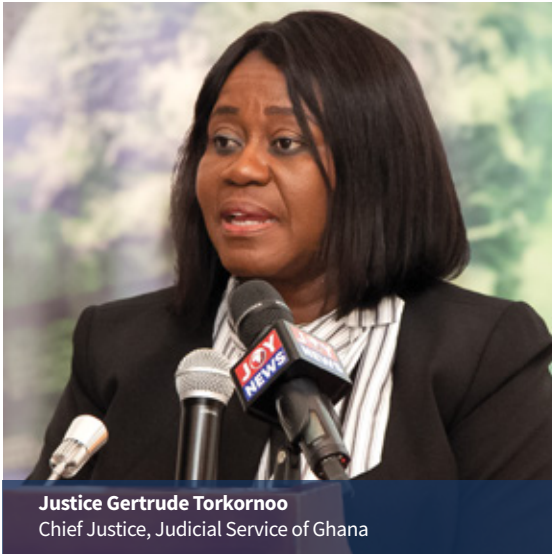
## Keynote Address

### Justice Gertrude Torkornoo

Chief Justice, Judicial Service of Ghana

In her remarks, Her Ladyship, Chief Justice of the Republic of Ghana, Justice Gertrude Torkornoo, thanked the CSA for supporting the Judicial Service in handling cybercrime issues. She further indicated that to ensure success in the prosecution and adjudication of cybercrimes involving electronic evidence, the judiciary and other criminal justice sector actors must have the requisite resources. Training workshops should therefore be consistently organised to build the capacity of the judiciary to understand the ever-changing issues and trends surrounding cybercrimes and the admissibility of electronic evidence, she explained.

She added that the Judiciary looks forward to collaborating with the CSA and other member



institutions of the JCC in implementing measures required to fight cybercrime through the adjudication of cybercrime cases and enhance the admissibility of electronic evidence in courts.

## Day 1

The first day of the workshop featured presentations covering internet and cybercrime fundamentals, digital and electronic evidence, and an overview of the international legal framework. Mr. Georges Van Eshof, a TAIEX Expert from the Netherlands emphasised the importance of gaining sufficient technological knowledge to enhance effectiveness in participants' roles. He simplified complex computer concepts, discussed internet components and services, and highlighted potential challenges posed by the dark web to criminal prosecution.

Ms. Esther George, the OCWAR-C Expert from the United Kingdom introduced participants to the information society and cybercrime, emphasising international efforts to combat modern criminality. She discussed various types of cybercrime, their impact, emerging threats and trends, and tools for addressing cyber threats.

Justice Afia Serwah Asare-Botwe, a trainer of trainers for the Council of Europe urged participants to expedite processes related to cases involving minors and children, emphasising sessions 62–66 of the Cybersecurity Act, 2020.

## Day 2 & 3

The second day of the workshop began with a presentation from the various facilitators. In the subsequent skills-building session, participants were asked to analyse a case study synopsis in groups of 4. Each group tackled a specific topic: "Who am I," "Follow the Data," "Follow the Money," and "Follow the Leader."

Day three entailed group presentations, where each of the four groups provided insights into their respective topics, including obtaining evidence for a prize-winning game, navigating requests to ISPs, and exploring electronic evidence related to financial transactions and international cooperation.

## Conclusion

The Acting Director, of Capacity Building and Awareness Creation, CSA, Mr. Alexander Oppong, in a brief remark on behalf of the Director-General, Dr. Albert Antwi-Boasiako, indicated that the workshop on cybercrime and electronic evidence highlighted the importance of understanding the complexities of cybercrime in the judicial system, hence it is essential to engage in ongoing education and collaboration to ensure justice is upheld in the digital age.

Participants were awarded certificates of participation at the end of the training.

## Recommendations

The following recommendations emerged from the workshop.

- Targeted cybercrime training for police prosecutors should be organised to aid in handling cybercrime cases.
- Politicians should be involved in subsequent engagements to aid in financing cybercrime cases.

# WORKSHOP ON THE LICENSING OF CYBERSECURITY SERVICE PROVIDERS, ACCREDITATION OF CYBERSECURITY ESTABLISHMENTS AND CYBERSECURITY PROFESSIONALS

## Background

As part of Ghana's efforts to ensure a culture of digital safety, the Cyber Security Authority (CSA) in collaboration with the Institute of ICT Professionals Ghana (IIPGH) organised a Virtual Workshop on the Licensing of Cybersecurity Service Providers (CSPs), the Accreditation of Cybersecurity Establishments (CEs) and Cybersecurity Professionals (CPs). The workshop presented a platform to provide clarity on the ongoing cybersecurity licensing and accreditation programme in the country.

### Remarks

**Emmanuel Gadasu**

Head of Data Protection, IIPGH

Mr. Emmanuel Gadasu in his remarks acknowledged the participants and appreciated the leadership of CSA for its insight. He spelt out the objective of NCSAM 2023 and the need to promote cybersecurity awareness among businesses, children, government, and the public.

### Presentation

**Jennifer Mensah**

Lead, Legal and Compliance, CSA

Ms. Jennifer Mensah delivered a presentation on "The Licensing of Cybersecurity Service Providers, Accreditation of Cybersecurity Establishments and

Cybersecurity Professionals" by explaining the legal basis for the exercise, the licensing and accreditation requirements and the need for CSPs, CEs and CPs to comply with the directive.

Furtherance to the legal requirements, Ms. Jennifer Mensah highlighted the benefits of the process to the CPs and CSPs which included professional visibility in the provision of services to Critical Information Infrastructures and Public Sector Institutions.

## Conclusion and Recommendations

In conclusion, the Head of Data Protection (IIPGH), Ms. Edith Esi Mould, urged the CSA to enhance awareness creation on the accreditation and licensing of CPs and CSPs and cybersecurity Establishments, (CEs). Mr. Emmanuel Gadasu recommended the CSA conduct continuous research on current trends in cyber accreditation and licensing and continuously improve the system. Mr. Sheriff Issah in his closing remarks expressed his gratitude to all participants and facilitators for joining in the workshop. He also commended the CSA for timely responses to addressing licensing and accreditation issues and encouraged all participants to apply for the licensing and accreditation as well as raise awareness on the correspondence.

# TWO-DAY CYBERSECURITY COLLABORATIVE WORKSHOP WITH NATIONAL PENSIONS REGULATORY AUTHORITY (NPRA)

## Background

As part of the measures to effectively promote a culture of digital safety, the Cyber Security Authority (CSA) leveraged on the 2023 edition of the annual National Cyber Security Awareness Month (NCSAM) to collaborate with members of the National Pensions Regulatory Authority (NPRA) to organise cybercrime and cybersecurity sensitisation engagements. The engagements were to ensure a heightened awareness of cybercrime and cybersecurity issues among CII member institutions, staff and stakeholders, leading to the prevention and mitigation of cybersecurity incidents.

In view of this, the National Pensions Regulatory Authority (NPRA) in collaboration with the Cyber Security Authority organised a 2-day Cybercrime/Cybersecurity Sensitisation and Awareness Creation Workshop for their staff in Accra.

The first day of the workshop hosted the senior management members and zonal staff of NPRA. The second day hosted the middle management staff, junior management staff, and national service personnel of NPRA.

### Opening Remarks

#### Hayford Attah Krufi

Chief Executive Officer, National Pensions Regulatory Authority (NPRA).

Mr. Hayford Attah Krufi expressed appreciation to the CSA for the workshop and emphasised the importance of cyber resilience in their industry for business continuity in the event of cyberattacks. He acknowledged that the Cybersecurity Act, 2020 (Act 1038) which established the CSA gave it the mandate to educate the public on matters relating to cybercrime and cybersecurity and to build the capacity of persons in the public and private sectors on matters related to cybersecurity. He highlighted that the NPRA is one of the designated CII



institutions, and that should their institution suffer any online data breaches, it will critically affect the country. Mr. Krufi urged all the members of staff to take the cybersecurity training seriously to ensure data safety from cyberattacks.

## Presentations

Cyber Security Authority Officials

Mr. Gerald Awadzi and Mr. Joseph Attah from the CSA facilitated the capacity building exercises. They took the participants through the modus operandi of different forms of online fraud which included investment fraud, romance scams, recruitment scams, and shopping scams and how they can be prevented. Online blackmail such as extortion and sextortion, unauthorised access, which included account takeover and phishing, online impersonation, information disclosure and Online Child Sexual Exploitation and Abuse (OCSEA), ransomware, and misinformation were also among the areas the participants were engaged in.

The participants were further urged to ensure password hygiene, enable multi-factor or two-factor



authentication on their devices and applications, regularly update software and systems, enhance secure browsing habits, avoid public Wi-Fi, and use anti-virus.

Issues related to cybersecurity and CII institutions, the types of cybersecurity threats, malware, social engineering, and phishing were emphasized. The participants were then taken through cybersecurity best practices for personal devices and social media security, and channels through which cyber-related incidents can be reported.

Participants were given a poll of questions to answer to get their understanding of cyber-related issues. They were taken through how to secure their devices and restrict other applications from accessing their location.

Discussing some risks associated with social media usage, such as identity theft, reputational damage, malware, phishing, online impersonation, and

cyberstalking, participants were further taken through some safety tips such as enforcing strong privacy settings, keeping personal and professional profiles separate, not sharing sensitive information, being cautious of friend requests and direct messages, using a strong and unique password, avoiding using the same password for multiple accounts, staying up to date on security issues, and enabling multi-factor authentication.

## Conclusion

The workshop was well appreciated and considered effective in helping in the prevention and mitigation of cybersecurity incidents. It was suggested that similar workshops should be organised for the board members of NPRA.



## CYBER DRILLS ON INCIDENT RESPONSE

The National Computer Emergency Response Team (CERT) of the Cyber Security Authority held a tabletop exercise (Cyber Drill) on Distributed Denial of Service (DDoS) Attack for the sectoral CERTs as part of activities to mark the National Cyber Security Awareness Month (NCSAM). The event was attended by officers of the Ghana Armed Forces, National Communications Authority (NCA), National Signals Bureau (NSB), Data Protection Commission (DPC), National Information Technology Agency (NITA) and the Ghanaian Academic and Research Network (GARNET).



Explaining the rationale for the exercise, the Lead at the National CERT at the CSA, Mr. Stephen Cudjoe-Seshie, said the core objective was to examine the preparedness of the National and Sectoral CERTs to protect against, identify, detect, respond to, and recover from a disruptive Distributed Denial of Service (DDoS) attack by:

- examining the preparedness of Sectoral CERTs to protect themselves and their constituents from a DDoS attack,
- examining the information sharing protocols of Sectoral CERTs with internal and external stakeholders and partners, including commercial service providers,
- reviewing the reporting protocols of Sectoral CERTs considering the provisions of the Cybersecurity Act, 2020 (Act 1038), and
- assessing the communications plans of Sectoral CERTs to respond to inquiries from the public regarding a DDoS attack.

Prior to the actual cyber drill, a Principal Engineer at NETSCOUT engaged the participants in a virtual session to present the latest trends in DDoS attacks. NETSCOUT is a trusted leader in DDoS protection solutions that has its headquarters in Westford, Massachusetts, USA.

Some of the participants who shared their thoughts at the end of the session regarded the exercise as insightful and very educational, emphasising that it had provided them with an opportunity to construct a network of contacts to help them with their work.

# 05.

## The National Cybersecurity Challenge (NCC)





# THE NATIONAL CYBERSECURITY CHALLENGE (NCC)

## Background

The National Cybersecurity Challenge (NCC) is an initiative of the Cyber Security Authority to promote cybersecurity awareness among Senior High School students.

This year's challenge featured the participation of 50 senior high schools from across the nation. The schools were divided into four zones: Northern, Southern, Eastern, and Middle. Ultimately, the winners from each zone advanced to compete in the finals.

The participating schools in the 2023 NCC finals were: Wesley Girls' High School, Navrongo Senior High School, Ola Girls' Senior High School, and Prempeh College. Other students from Unity International College, Fafraha Community Senior High School, St. Dominic Junior High School, West Africa Senior High School, and Bishop Herman Senior High School were also present to support their colleagues.



The Winning Trophy







**Mercy Araba Kertson**  
Ag. Director of Administration

## Welcome Address

**Mercy Araba Kertson**  
Ag. Director of Administration

The Ag. Director of Administration at the CSA, Madam Mercy Araba Kertson delivered the welcome address on behalf of the Director-General and commended management and school authorities who prepared the students for the exercise. She noted that the NCC will be an annual rallying point for high school students across the country to compete in exciting exercises demonstrating their knowledge of cybersecurity, and the threats of the internet. She concluded her remarks by wishing the competing schools and students a happy and educative challenge.



**Lucia Soleti**  
UNICEF, Chief Child Protection Official

## Remarks

**Lucia Soleti**  
UNICEF, Chief Child Protection Official

Lucia Soleti applauded the CSA for the tremendous effort in protecting children online. She shared statistics from the National Centre for Missing and Exploited Children which notes that 22,000 cyber reports related to child sexual abuse materials were accessed, shared, or produced from Ghana, adding that the National Cybersecurity Challenge is a good platform for engaging and equipping children and young people to actively adopt safe practices whilst online. She encouraged the government to develop an industry code that covers specific issues relevant to child online protection.

## Remarks

**Benard Asamoah**  
Country Head, UNODC, Ghana

Mr. Asamoah noted that the National cybersecurity challenge is not just a recognition of individual achievement but a testament to the collective commitment towards promoting a culture of digital



**Benard Asamoah**  
Country Head, UNODC, Ghana

safety in Senior High Schools, adding that “Promoting a Culture of Digital Safety” underscores the critical need for cultivating awareness, knowledge sharing, and skills to protect the digital ecosystem from evolving trends. He therefore encouraged all stakeholders to work in unison to fight cybercrime.



**Prince Sarpong**  
Chief Information Officer, AT Ltd

## Remarks

### Prince Sarpong

Chief Information Officer, AT Ltd

Mr. Sarpong stated that AT Ghana is working hand in hand with the security agencies to ensure that cyber threats are dealt with and the information needed to take down perpetrators is also provided on time to track them down.



**Gabriel Appiah**  
Vice President, Ghana Internet Safety

## Remarks

### Gabriel Appiah

Vice President, Ghana Internet Safety

Mr. Appiah noted that Ghana has taken commendable steps in promoting online safety, particularly for children. He requested for a collective effort from industry, civil society organisations and private organisations to support the goal of child online safety.



**Robert Nunoo**  
General Manager, Innovare Limited

## Remarks

### Robert Nunoo

General Manager, Innovare Limited

In his remarks, Mr. Nunoo expressed Innovare’s appreciation to be a part of the event’s sponsors. He congratulated all participating schools and offered them his best wishes.



## The Competition

Four schools competed for the National Cybersecurity Challenge trophy, comprising the winners from the four (4) zones, with Mr. Joseph Quaye from the E-Crime Bureau as the quiz master.

The competition was divided into four rounds. The first round was made up of forty questions, a combination of multiple-choice questions where each school was required to answer a total of ten questions. The second round consisted of riddles for each school to unravel. The third and final rounds was a practical session, where students were equipped with skills to conduct investigations leveraging open-source intelligence.

At the end of the competition, Ola Girls' Senior High School won with a total score of forty-five (45), the second position was a tie between Wesley Girls Senior High School and Prempeh College, with a score of thirty-eight (38) points, and Navorongo Senior High School came in third with thirty-four (34) points.



## Awards Ceremony

The Awards Ceremony took place at the Kempinski Hotel Gold Coast as part of the closing ceremony of the Global Conference on Cyber Capacity Building (GC3B). Awards were presented by the Minister for Communications and Digitalisation, Honourable Ursula Owusu-Ekuful and the Director General of the Cyber Security Authority, Dr. Albert Antwi-Boasiako.

Winners for the 2023 edition of NCC, Ola Girls' Senior High School were awarded a cash prize of GH¢ 7,000.00, a trophy, branded souvenirs, a laptop and certificates of participation. Prempeh College and Wesley Girls' Senior High School were each presented with a cash prize of GH¢ 3,500.00, branded souvenirs, a laptop and certificates of participation. The third runner-up, Navorongo Senior High School received a cash prize of GH¢ 2,000.00, branded souvenirs, a laptop and certificates of participation.



# 06.

## Cybersecurity Collaborative Workshops





# CYBERSECURITY COLLABORATIVE WORKSHOPS

## Background

The 2023 National Cyber Security Awareness Month (NCSAM) celebration featured collaborative cybersecurity workshops tailored for various institutions aimed at fostering awareness and preparedness against cyber threats. With a focus on fostering a culture of cybersecurity consciousness, the workshops brought together diverse stakeholders from academia, industry, government and private sectors and provided a platform for participants to engage in interactive discussions, hands-on exercises, and knowledge-sharing sessions. Participants from the institutions gained valuable insights into emerging cyber threats and were taken through proactive measures to safeguard digital assets as well as sensitive data. As a cornerstone of NCSAM 2023, the workshops covered the collective responsibility to fortify cyber resilience and to promote a safer digital ecosystem for all.

Below are the beneficiary institutions of the collaborative workshops:

- Prosecuting State Attorneys (Department of Public Prosecutions)
- Ghana Civil Service
- National Identification Authority
- Ghana Shippers Authority
- Ghana Maritime Authority
- Ghana Communications Technology University (GCTU)
- Kwame Nkrumah University for Science and Technology (KNUST)
- Ghana Institution of Engineering
- Hubtel
- CalBank PLC
- Association of Ghana Industries
- Enterprise Group
- Star Assurance
- Access Bank
- Genius IT Foundation

## Capacity Building Workshop for Prosecuting State Attorneys (Department of Public Prosecutions)

A virtual awareness creation session was held for Prosecuting State Attorneys as part of the 2023 edition of the NCSAM.

Participants were introduced to the role and responsibilities of the Cyber Security Authority, highlighting its mandate, and outlining various cybersecurity threats faced by individuals, including malware, social engineering, and phishing. Best practices for self-protection when using social media and personal devices were shared, with a warning against using open or unknown public Wi-Fi for private or sensitive transactions. Provisions in the law that criminalise certain risks faced by children in the Cyber Security Act, 2020 (1038) were discussed. The significance of cybersecurity incident reporting, particularly in the realm of criminal justice, was also underscored, emphasising its pivotal role in maintaining a secure digital space.

## Cybersecurity Collaborative Workshop with Ghana Civil Service

The Cyber Security Authority organised a sensitisation event for the staff of the Head of Civil Service (OHCS) aimed to raise awareness of the importance of maintaining cyber hygiene among public institutions through comparable training exercises.

It was pointed out during the training that human weaknesses on the internet could not be avoided given the convenient services available to citizens because of the government's drive towards digitalisation, hence the imperative need for constant education on cybersecurity.

Participants were taken through the types of cyber incidents, including ransomware and malware, and offered useful tips for protecting a digital system such as encryption, multi-factor authentication, regular system updates, the installation of software, and the constant review of app permissions.

## Cybersecurity Collaborative Workshop with National Identification Authority (NIA)

The National Identification Authority (NIA) in collaboration with the Cyber Security Authority (CSA) organised a sensitisation workshop for their staff. The event comprised virtual and in-person sessions, allowing participation of staff in different regions across the country.

The participants were educated on the four pillars of the Safer Internet Ghana awareness creation campaign - Children, the Public, Businesses, and the Government. The NIA is a government institution that holds very sensitive data hence the staff were educated on the importance of using genuine anti-virus/anti-malware protection on mobile devices, given the sensitive data accessed on these devices.

Key elements of cybersecurity were delved into such as the repercussions of online impersonation citing instances of high-profile individuals falling victim to identity theft. Participants were guided on how to recognise phishing emails and how to set robust passwords.

Prevalent cyber threats were also discussed and participants urged to exercise caution in their online dealings.

## **Cybersecurity Collaborative Workshop with Ghana Shippers Authority**

A hybrid session was held by the Ghana Shippers Association (GSA) in collaboration with the CSA to expose the staff of the GSA to cybersecurity trends, threats, and preventive measures.

It was noted during the session that criminals exploit the human factor, through social engineering, in the cyberspace to attack organisations and individuals. Various global and domestic cybersecurity incidents were highlighted, including the hacking of the systems of the Electricity Company of Ghana, which impacted the power supply in many areas of the country.

Some of the contributory factors to data breaches in organisations were identified as human error, outdated software, poor password hygiene, weak network security, and insider threats.

Regarding mobile device security, participants were advised to enable data encryption, enable remote wipe capabilities, set up two/multi-factor authentication, regularly update software, and avoid using free or public Wi-Fi for sensitive transactions.

A demonstration on checking the strength of passwords and ensuring the safety of email accounts was conducted to conclude the session.

## **Cybersecurity Collaborative Workshop with Ghana Maritime Authority**

The virtual workshop, aimed at promoting awareness of cybersecurity threats in institutions, was organised by the Ghana Maritime Authority (GMA) in collaboration with the CSA. The sensitisation event was used to educate the staff of the GMA about common cyber threats such as malware, phishing, data breaches, protecting individual and individual digital assets, and best practices for online safety.

Participants were educated on securing mobile devices, enabling data encryption, setting up multi-factor authentication, and regular device updates. Participants were advised to avoid using free public Wi-Fi, especially for sensitive transactions.

Common hacker tactics, such as fake shops and social media account takeovers, were addressed following which relevant statistics from the Computer Emergency Response Team of CSA were cited, highlighting the Authority's efforts in handling prevailing cyber issues reported by the public.

It was explained to participants that global trends of cybercrimes and operations of hackers have damaging individual and national implications, and hence the need to be vigilant in cyberspace.

## **Cybersecurity Collaborative Workshop the Ghana Communications Technology University (GCTU)**

A "Cyber Security Awareness Day" event aimed at providing valuable insights on how to safeguard information assets and stay secure online was organised for members of the Ghana Communications Technology University as part of the 2023 National Cybersecurity Awareness Month (NCSAM) celebration.

They were educated on known threats such as financial fraud, with emphasis placed on the critical need to empower every member of the academic community with the knowledge and skills required to navigate the cyberspace securely.

Prevalent global cyber threats were discussed and participants were urged to enhance their cybersecurity by installing security software and ensuring regular updates of their devices.

A team from the CSA who facilitated the workshop encouraged the participants to prioritise the pursuit of cybersecurity education with utmost seriousness, underscoring its pivotal role in safeguarding their online activities.

## **Cybersecurity Collaborative Workshop with students of the Kwame Nkrumah University of Science and Technology (KNUST)**

A webinar to enlighten students on the importance of digital safety and the need to practice cyber hygiene was organised for students of the Kwame Nkrumah University of Science and Technology (KNUST).

The theme for NCSAM 2023, "Promoting a Culture of Digital Safety" was discussed, emphasising the role of individuals, institutions, and government in fostering digital safety. Key points addressed included the importance of digital safety, vulnerability, privacy concerns, economic impact, trust, and reputation. Additionally, the need for institutions to provide frequent employee training, investing in cybersecurity, and developing policies to address incident attacks and vendor security were accentuated.

Furthermore, the role the government is playing in building a culture of digital safety through regulations and legislation in cybersecurity and the fact that individuals have a greater responsibility to ensure they stay safe online were highlighted.

## **Cybersecurity Collaborative Workshop with the Ghana Institution of Engineering**

A hybrid awareness creation session was conducted for the staff of the Ghana Institution of Engineering to mark the National Cybersecurity Awareness Month 2023.

The members of the Institute were educated on threats and vulnerabilities faced by individuals and businesses and the modus operandi employed by mobile money fraudsters.

General safety tips, advisories, and best practices for cybersecurity including avoiding public wifi, using

strong passwords, and doing due diligence before doing business online were discussed. They were further cautioned that the modus operandi of cybercriminals evolved, hence the importance to be being extra vigilant to avoid falling prey to scams.

The session ended with a call for participants to report suspicious activities to the Cyber Security Authority's cybercrime/cybersecurity incident reporting points of contact on 292.

## **Cybersecurity Collaborative workshop with the staff of Hubtel Ghana**

The primary goal of the sensitisation event was to educate Hubtel staff about prevalent cybercrimes and threats. The presentations were tailored around safeguarding both individual and collective digital assets.

Touching on global cybercrime trends, the staff were taken through instances of cyberattacks on nations which triggered a state of emergency due to a shortage of essential commodities.

Facilitators of the session emphasised the fundamental components that constituted the essence of cybersecurity: People, Processes, and Technology and underscored the critical role that staff play as both defenders and potential targets within their organisations.

## **Cybersecurity Collaborative Workshop with the staff of CalBank Ghana**

The Cyber Security Authority collaborated with CalBank to create awareness of cybersecurity for its staff and customers through an virtual and in-person session.

Major highlights of the session included education on responsible social media usage, adjusting privacy settings, and risks of oversharing personal information online. Tips for secure online shopping were provided, and the need to deal with reputable



websites and secure connections. The participants were further cautioned against using public Wi-Fi for financial transactions.

The session also focused on educating participants on trending cybersecurity threats such as social engineering, phishing, fake mobile banking apps, phone theft, and keylogging malware. Recommendations for cyberspace safety were outlined and included using anti-malware protection, implementing multi-factor authentication, and regularly updating applications and operating systems.

Participants were educated on online behaviours that increase susceptibility to cyber attacks, such as visiting malicious websites, sharing sensitive information on public Wi-Fi, and using weak passwords.

## **Cybersecurity Collaborative Workshop with the Association of Ghana Industries**

The purpose of this hybrid sensitisation was to inform the Association of Ghana Industries about cybersecurity threats and how they can safely navigate and do business online.

Highlights of the engagement focused on how to protect individual and business digital assets, knowledge of best practices for online safety, the ability to recognise warning signs of cyberattacks and steps to take in mitigating them.

The risks associated with social media, such as identity theft, cyberstalking, online impersonation, malware phishing, and reputational damage, were discussed. Modes of operation used by hackers, including setting up fake shops, taking over social media accounts, credential harvesting through phishing links, online blackmail, and impersonating VVIPs for recruitment scams were also highlighted. Participants further received education on strategies for securing mobile devices, including enabling data encryption, remote wipe capabilities, multi-factor authentication, and regularly updating devices. Participants were advised to avoid using free public

Wi-Fi and to refrain from auto-logging on applications.

## **Cybersecurity Collaborative Workshop with staff of Enterprise Group**

The Cyber Security Authority in collaboration with the Enterprise Group organised an awareness creation session to sensitise and equip the staff of Enterprise Group on Cybersecurity developments and protective measures as part of for the National Cyber Security Awareness Month (NCSAM) for 2023.

The facilitators for the workshop, drawn from the Cyber Security Authority focused on the benefits of digitalisation while noting that it also poses security risks and hence urged caution. Participants were taken through some threats associated with the use of mobile devices and the security measures that must be implemented to prevent an attack or data breach.

## **Cybersecurity Collaborative Workshop with the staff of Star Assurance**

The virtual event was organised by Star Assurance with the primary objective to sensitise and conscientise their staff on cybersecurity in an ever-evolving global landscape of technology.

Members of the National Computer Emergency Response Team (CERT) of the CSA educated the participants on instances of cyber attacks on state institutions, the types and risks associated with malware, social engineering, data breaches, the risks associated with social media usage, among others. Discussions furthered on social media risks, encompassing identity theft, cyberstalking, reputational damage, malware, phishing, and online impersonation. Emphasis was placed on the importance of Multi-Factor Authentication (MFA) as a critical security measure for all systems and devices.

## Cybersecurity Collaborative Workshop with the staff of Access Bank Ghana

The Cyber Security Authority and the Access Bank, Ghana organised a virtual awareness session to conscientise and equip staff on how to identify, prevent and mitigate cyber threats and to protect customers' funds.

Key points mentioned covered the impact of technological innovations on the banking industry's cybersecurity posture, and the increased frequency and sophistication of cyber threats targeting the banking sector. This is to ensure proactive

cybersecurity strategies to protect sensitive financial data and to maintain customer trust.

Banking institutions were encouraged to show keen interest in the regulatory interventions for cybersecurity in the banking sector, including the licensing and accreditation of Cybersecurity Service Providers, Cybersecurity Professionals and Cybersecurity Establishments.

The CSA shared insights on the types of cyber threats, educating the staff on various cyber threats including malware, phishing, and social engineering, and cybersecurity best practices that ensure device and overall online safety.



Group pictures from the collaborative workshops

# Cyber Security Authority Collaborates with the Genius IT Foundation in the Volta Region

## Background

The 2023 National Cyber Security Awareness Month (NCSAM) celebration in the Volta region witnessed collaborative efforts between the Cyber Security Authority (CSA) and the Genius IT Foundation. The commemoration included lectures, seminars across institutions, and media engagements, culminating in the National Cybersecurity Awareness Conference 2023 at the St. Stevens Hotel in Ho.

Dignitaries from the various security services, the banking sector, government agencies, and other sectors participated in the event, with the Volta Regional Minister, Dr. Achibald Yao Letsa, in attendance.



**Dr. Archibald Letsa**  
Volta Regional Minister

## Keynote address

**Dr. Archibald Letsa**  
Volta Regional Minister

The Volta Regional Minister, Dr. Archibald Letsa, said in his keynote address that the region was geared up for technological advancement, hence the need for robust cybersecurity measures.

Highlighting the dynamic nature of the digital landscape, he underscored the constant evolution of

methods employed by cybercriminals to exploit the unsuspecting public. Dr. Letsa urged the public to be proactive by securing their vulnerabilities against the shenanigans of cybercriminals.

Quoting statistics from the 2021 National Population and Housing Census, the minister stated that the population of the Volta Region stood at about 1.6 million and is projected to grow by 1.8 million in 2025 and 2.1 million by 2030, with a growth rate of 2.1 percent.

“This demographic strength underscores the economic power of the region. However, without adequate cybersecurity measures, this growth could be jeopardised by cyber threats,” he added.

Dr. Letsa endorsed initiatives such as the National Cybersecurity Awareness Month, emphasising its critical role in promoting digital inclusiveness and education.

## Remarks

**Desmond Kitsi**

Executive Director and Founder, Genesis IT Foundation

Mr. Desmond Kitsi emphasised Africa's untapped potential and highlighted pressing challenges hindering technological harnessing for sustainable development, productivity, and wealth creation.

He reiterated the importance of cybersecurity and called for support from SMEs, the media, and the government to back cybersecurity awareness initiatives.

## Lecture

**Alfred Kumah**

Head of IT, University of Health and Allied Sciences

Mr. Alfred Kumah, the Head of IT at the University of Health and Allied Sciences, delivered a lecture emphasising the importance of safeguarding patients' data in the health sector. He highlighted the

potential risks in cybersecurity, including ransomware, data breaches, and inside threats, and stressed the need to implement measures to protect patient confidentiality.

## Lecture

**Bismark Tay**

Leadership and Management Consultant

Mr. Bismark Tay, a leadership and management consultant, highlighted the rise of cyberbullying in the educational sector, underscoring its potential impact on mental health. He advocated for measures such as firewalls to counter hostility arising from leaked educational content.

## Lecture

**Eric Aggor-Ohene**

Zenith Bank

In his lecture, Mr. Eric Aggor-Ohene indicated that in the pursuit of financial security, the trust placed in banks hinges on robust cybersecurity and alluded to the critical role of safeguarding against malware, viruses, and data theft in the face of escalating cyber threats.

With the banking sector as a prime target due to large transaction volumes and complex client needs, Mr. Aggor-Ohene stated that individual responsibility for safety is paramount and that, despite being highly regulated, the sector requires initiative-taking measures from clients.

He underscored the urgency of protecting personal information and the need for individuals to secure their email accounts and PIN codes.

## Lecture

**Eric Kafui Bansah**

Cyber Security Authority

Mr. Bansah in a lecture underscored the heightened risks in the digital realm, citing cyber threats such as cyberbullying, sextortion, online fraud, and misinformation impacting both individuals and organisations.

According to him, Ghana's global rank of 13th in



internet usage time calls for vigilant measures to counter increased exposure to cyber threats.

Mr. Bansah advocated for awareness creation and capacity building in line with the dictates in Section (60) of the Cybersecurity Act, 2020, adding that prioritising cybersecurity involves recognising phishing emails, promoting secure online behaviour, and implementing crucial measures such as robust access controls, strong passwords, multi-factor authentication, and updated software inventories for overall organisational security.

He called on Ghanaians to, as a matter of urgency, dial 292 for prompt response measures to effectively minimise potential harm in the occurrence of cyber incidents and attacks.

## Lecture

**Dennis Duncan**

Fraud, cybersecurity, and Forensics Experts  
Investigation Bureau

Mr. Dennis Duncan, a seasoned private investigator, delivered a message on safety, urging the public to stay security-conscious and vigilant.

He spoke about the importance of controlling shared information and being mindful of potential risks, and he lauded the National Cybersecurity Awareness Month, describing it as a significant success.



# 08.

| **Media Engagements**



## NCSAM 2023 Media Engagements

MEDIA HOUSE	TOPIC	OFFICER
GHOne TV	Weakest links in cybersecurity	Alexander Oppong
Joy News	Licensing and Accreditation	Jennifer Mensah & Benjamin Ofori
Joy FM	Mission of NCSAM/related activities	Stephen Cudjoe-Seshie
UTV	Mandate of COP/ achievements	Nelson Gerald Darko
TV XYZ/Power FM	Cybersecurity awareness	Isaac Socrates Mensah
Joy FM	Safety in cybersecurity	Stephen Cudjoe-Seshie
Darling FM	Staying safe online	Isaac Socrates Mensah & Mary Ama Bawa
Eagle FM	Cybersecurity Awareness	Mary Ama Bawa
Obuoba FM	Online Vigilance	Patricia Adafienu & Mary Ama Bawa
Max FM	Staying protected	Mary Ama Bawa
Radio Central	Cybersecurity education	Mary Ama Bawa
TV XYZ/Power FM	Child Online Protection education	Nelson Gerald Darko
Empire FM	Cyber awareness month	Mary Ama Bawa
Joy FM	NCSAM education	Mary Ama Bawa
TV XYZ/Power FM	Cybersecurity Awareness	Nelson Gerald Darko
Joy FM	Cybersecurity Education	Mary Ama Bawa
Adom FM	Cybersecurity consciousness	Joseph Attoh
Cape FM	Staying ahead	Mary Ama Bawa & Joseph Attoh
Asaase Radio	What to look out for to stay cyber secure	Stephen Cudjoe-Seshie
Kasapa FM	Cybersecurity Awareness	Mary Ama Bawa
Atinka FM	Cybersecurity Advisories	Mary Ama Bawa
Kessben FM	Tips for staying secure online	Mary Ama Bawa
Live FM	Online protection	Mary Ama Bawa
Ark FM	Cybersecurity Education	Mary Ama Bawa

## Participation Analysis

S/N	EVENT	GUESTS
1	Media Launch of the National Cyber Security Awareness Month (NCSAM) 2023 (Hybrid)	3,409
2	Capacity Building Workshop for Prosecuting State Attorneys (Department of Public Prosecutions)	65
3	The Launch of Ghana Armed Forces Cyber Security Awareness Month (Ghana Armed Forces)	150
4	Official Launch of the National Cyber Security Awareness Month (NCSAM) 2023 (Hybrid)	1,656
5	Cybersecurity Collaborative Workshop with Ghana Civil Service	74
6	Cybersecurity Collaborative Workshop with National Identification Authority	1, 562
7	NSB Internal Launch of Cybersecurity Awareness Month (National Signals Bureau (NSB))	35
8	Webinar on Data Protection Awareness for the Public (Data Protection Commission (DPC))	250
9	Workshop on Critical Information Infrastructure (CII) Security and Risk Management (In-person)	115
10	Sensitisation Workshop on Cyber Security (Financial Intelligence Centre (FIC))	35
11	Cybersecurity Collaborative Workshop with IIPGH	167
12	Consultative Workshop on the Development of the Accreditation Framework to Accredite Sectoral Computer Emergency Response Teams (CERTs) (In-Person)	40
13	Cybersecurity Sensitisation for Executive Members of Customs / and Cyber Security Sensitisation for Staff of GRA and Customs (Ghana Revenue Authority (Customs))	60
14	Cybersecurity Collaborative Workshop with Ghana Shippers Authority	35
15	Cybersecurity Collaborative Workshop with National Pensions Regulatory Authority (NPRA)	130
16	Cybersecurity Collaborative Workshop with Ghana Maritime Authority	60
17	Cybersecurity Collaborative Workshop with Ghana Communications Technology University (GCTU)	350
18	Cybersecurity Collaborative Workshop with Kwame Nkrumah University for Science and Technology (KNUST)	45
19	Cybersecurity Collaborative Workshop with the Institute of Engineers	50
20	Cybercrime/Cybersecurity Sensitisation and Awareness Creation Workshop (Ghana Prisons Service)	95
21	Impact of Disinformation on Electoral Integrity, Peace and Security (Hybrid)	200
22	Cybersecurity Collaborative Workshop with MTN Ghana	534
23	Cybercrime and Cybersecurity Sensitisation Engagement (Economic and Organised Crime Office (EOCO))	80
24	Legislative Instrument Validation Meeting	26
25	Cybersecurity Collaborative Workshop with CalBank PLC	62

S/N	EVENT	GUESTS
26	Introductory Course on Cybercrime and Electronic Evidence for Judges and Prosecutors in Ghana (In-Person)	115
27	Sectoral CERT Update Workshop (In-Person)	36
28	Cybersecurity Collaborative Workshop with Hubtel	301
29	Workshop on Data Management and Usage	70
30	Cybersecurity Collaborative Workshop with the Association of Ghana Industries	56
31	Cyber Drills on National Incident Response (In-Person)	20
32	Promoting Cybersecurity Consciousness among Research Department Staff	70
33	Stakeholder Engagement with Cybersecurity Service Providers	79
34	Stakeholder Engagement with Cybersecurity Establishments	68
35	Cybersecurity Collaborative Workshop with Genius IT Foundation	1,500
36	Cybercrime and Cybersecurity Sensitisation for Staff of the Ministry of National Security (MNS)	85
37	Stakeholder Engagement with Cybersecurity Professionals	150
38	Cybersecurity Workshop for Directors of National Investigations Bureau (NIB)	63
39	Cybersecurity Collaborative Workshop with Enterprise Group	175
40	Cybercrime and Cybersecurity Sensitisation Engagement - Narcotics Control Commission (NACOC)	70
41	Cybersecurity Collaborative Workshop with Star Assurance	150
42	Cybersecurity Collaborative Workshop with Access Bank	822
43	Cybercrime and Cybersecurity Sensitisation Engagement for staff of Ghana Fire Service	85
44	Workshop on the Role and Impact of Cybersecurity Governance in the Protection of Critical Information Infrastructure (In-person)	82
45	Report on the Cybersecurity regulation and the readiness of state-owned enterprises	30
46	National Cybersecurity Challenge- Middle Zone	350
47	National Cybersecurity Challenge – Southern Zone	300
48	National Cybersecurity Challenge- Eastern Zone	400
49	National Cybersecurity Challenge – Northern Zone	600
50	National Cybersecurity Challenge- Finale	550
Total Number of guests		15,512



# National Cyber Security Awareness Month (NCSAM) 2023

## Planning & Steering Committee

### Steering Committee Leadership

- i. Hon. Ama Pomaa Boateng, MoCD
- ii. Dr. Albert Antwi-Boasiako, CSA

### Programmes and Content

- i. Benjamin Ofori
- ii. Aaron Felix Opoku Boateng
- iii. Felix Afedi
- iv. Godfred Kumi Kwakye
- v. Afia Darko Asante

### Budget and Logistics

- i. Johnson Awua
- ii. Abigail Esi Otabil
- iii. Kwabena Adu Agyei
- iv. Duke Banson
- v. Adwoa Noonoo Assan

### Media and Communications

- i. Mary Ama Bawa
- ii. Faustina Maner Angmor
- iii. Erik Gordon-Quaicoe
- iv. Sharon Paulina Boye

### Collaborations and Partnerships

- i. Stephen Cudjoe-Seshie
- ii. Jael Bempah Amponsah
- iii. Adjoa Tabi-Asiamah
- iv. Henrietta Asamoah
- v. Emmanuella Darkwah

### Dignitaries and Protocol

- i. Mercy Araba Kertson
- ii. Osei Baah
- iii. James Dunyo
- iv. Augustus Francis Lamptey
- v. Eno Brago Attrams

### Industry Joint Programmes

- i. Isaac Socrates Mensah
- ii. Gerald Elorm Awadzi
- iii. Joseph Antwi Attah

### Specific Initiative

- i. Eno Brago Attrams
- ii. Nelson Herald Darko
- iii. Alexander Awere-Kyere

### Appreciation/Acknowledgment team

- i. Alexander Oppong
- ii. Abigail Esi Otabil
- iii. Sarah Owusu

### Coordinating Team

- i. Alexander Oppong
- ii. Eric Kafui Bansah
- iii. Patricia Adafienu
- iv. Jael Bempah Amponsah

## Editorial Team

### Rapporteurs

- i. Sharon Paulina Boye, Lead
- ii. Abigail Kaki Onyame
- iii. Sherrifa Awinbun Atangiba
- iv. Priscilla Oppon
- v. Jael Amponsah Bempah
- vi. Naa Aku Shika Anum
- vii. Andrew Kissiedu-Asamoah
- viii. Kwame Forchie Boafo
- ix. Eric Mireku Danquah
- x. Zakia Wesoamo Bukari
- xi. Celestine Esi Adzayi

### Editors

- i. Mary Ama Bawa
- ii. Faustina Maner Angmor
- iii. Sebastian Syme
- iv. Cynthia M. Dassinor
- v. Sharon Paulina Boye
- vi. Eric Kafui Bansah
- vii. Patricia Adafienu
- viii. Anna Y. Awuku
- ix. Amanda Adade
- x. Zakia W. Bukari
- xi. Vivian Doh

### Graphic Design and Photography

- i. Eric Obeng Asante
- ii. Sharon Paulina Boye
- iii. Erik Gordon-Quaico



# PHOTO GALLERY

NATIONAL CYBER SECURITY AWARENESS MONTH



## Media Launch Of National Cyber Security Awareness Month (NCSAM) 2023









## Official Launch of the 2023 Edition of the National Cyber Security Awareness Month













## Launch of Cyber Security Awareness Month for the Personnel of the Ghana Armed Forces



## Sectoral CERTs Updates Workshop





**Workshop on the Role and Impact of Cybersecurity Governance in the Protection of Critical Information Infrastructure (CII)**



## Introductory Course on Cybercrime and Electronic Evidence for Judges in Ghana





# Two-day Cybersecurity Collaborative Workshop with National Pensions Regulatory Authority (NPRA)



## Workshop on Cybersecurity Sensitisation for the Staff of Financial Intelligence Centre (FIC)





## Cybercrime and Cybersecurity Sensitisation Engagement (Economic & Organised Crime Office (EOCO))





## The National Cybersecurity Challenge (NCC)





## Partners



# Sponsors





# CYBER SECURITY AUTHORITY (CSA)



Tel: +233303972530/1  
Email: [info@csa.gov.gh](mailto:info@csa.gov.gh)  
Digital Address: GL-126-7029

Cyber Security Authority Ghana  
3rd Floor, NCA Tower, KIA,  
6 Airport By-pass Road, Accra

[www.csa.gov.gh](http://www.csa.gov.gh)

     Cyber Security Authority Ghana