CYBER SECURITY AUTHORITY
(CSA)

ANNUAL REPORT 2022

www.csa.gov.gh

A SAFER DIGITAL GHANA

CYBER SECURITY AUTHORITY
FREEDOM AND JUSTICE
CSA

TABLE OF CONTENT

TABLE OF CONTENT

Acronyms

AfriSIG	African School on Internet Governance
ASID	Africa Safer Internet Day
AU	African Union
BoG	Bank of Ghana
CAMFED	Campaign for Female Education
CBAC	Capacity Building and Awareness Creation
CBAS	College of Basic and Applied Sciences
CCI	Commonwealth Cybercrime Initiative
CEIBS	China Europe International Business School
CERT	Computer Emergency Response Team
CERT-GH	National Computer Emergency Response Team
CEs	Cybersecurity Establishments
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
COE	Council of Europe
COP	Child Online Protection
CPs	Cybersecurity Professionals
CSA	Cyber Security Authority
CSOs	Civil Society Organisations
CSP+	Certified Security Principles+
CSPs	Cybersecurity Service Providers
CTS	Cybersecurity Technology Standards
DRIF	Digital Rights Inclusion Forum
ECG	Electricity Company of Ghana
ETC	Entity Tender Committee
EU	European Union
FIRST	Forum of Incident Response and Security Teams
FOC	Freedom Online Coalition
GAB	Ghana Association of Banks
GCI	Global Cybersecurity Index
GCIG	Global Commission on Internet Governance
GCNet	Ghana Community Network Service Limited
GDIs	Government Digitalisation Initiatives
GFCE	Global Forum for Cyber Experts
GIFCT	Global Internet Forum to Counter Terrorism
GLACY+	Global Action on Cybercrime Extended
HM-DEAA	Harmonised Model for Digital Evidence Admissibility Assessment

ICT	Information and Communication Technology
IFC	International Finance Corporation
IFSEC	International Fire and Security Exhibition and Conference
IGF	Internally Generated Funds
INTIC	National Information and Communications Technology Institute of Mozambique
ISACA	Information Systems Audit and Control Association
JCC	Joint Cybersecurity Committee
JD	Job Description
LECO	Legal & Compliance
LELU	Law Enforcement Liaison Unit
LI	Legislative Instrument
MFWA	Media Foundation for West Africa
MNR	Model National Response
MOUs	Memoranda of Understanding
MP	Member of Parliament
NCA	National Communications Authority
NCC	Narcotics Control Commission
NCPS	National Cybersecurity Policy and Strategy
NCSA	National Cyber Security Authority
NCSAM	National Cyber Security Awareness Month
NITA	National Information Technology Agency
OEWG	Open-Ended Working Group
PFM	Public Financial Management
PoC	Points of Contact
PSC	Public Services Commission
RTC	Regional Technical Committee
RTP	Restrictive Tendering Procedure
SOC	Security Operations Centre
SSB	Social Security Bank
SSNIT	Social Security and National Insurance Trust
TaT	Tech against Terrorism
TFDE	Task Force on Digital Equality
UNCTAD	United Nations Conference on Trade & Development
UNICEF	United Nations International Children's Emergency Fund
UNODC	United Nations O¬ice on Drugs & Crime
USA	United States of America

BRIEF OVERVIEW OF THE CYBER SECURITY AUTHORITY

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

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

MANDATE OF THE AUTHORITY

As a government agency under the Ministry of Communications and Digitalisation, the CSA has the responsibility to;

- Regulate cybersecurity activities in the country;
- Prevent, manage and respond to cybersecurity threats and cybersecurity incidents;
- Regulate owners of critical information infrastructure in respect of cybersecurity activities, cybersecurity service providers and practitioners in the country;
- Promote the development of cybersecurity in the country to ensure a secured and resilient digital ecosystem;
- Establish a platform for cross-sector engagement on matters of cybersecurity for effective co-ordination and co-operation between key public institutions and the private sector;
- Create awareness of cybersecurity matters; and
- Collaborate with international agencies to promote the cybersecurity of the country.

Vision

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.

Core Values

Confidentiality

Integrity

Reliability

Inclusiveness

Commitment

Professionalism

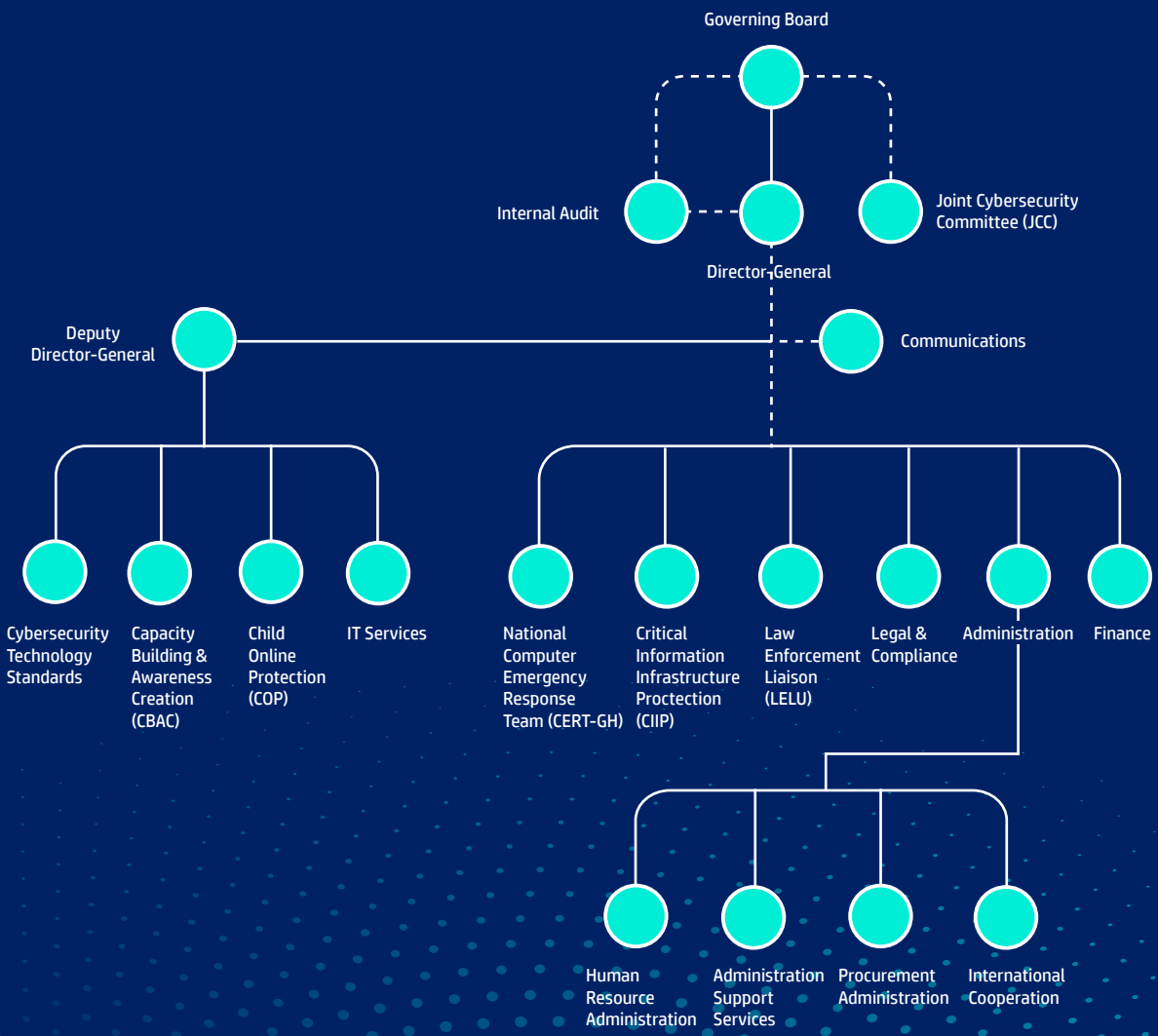
FUNCTIONS OF THE AUTHORITY

Pursuant to Section 4 of Act 1038, the CSA performs the following functions among others:

Advise	Government & public institutions on all matters related to cybersecurity in the country
Monitor	Cybersecurity threats within and outside the country
Respond	To cybersecurity incidents within and outside the country
Identify	CII Owners and advise the Minister on regulation of owners of CII
Promote	The protection of children online
Issue	Licences for the provision of cybersecurity services
Educate	The public on matters related to cybercrime and cybersecurity
Build	The capacity of persons in private and public sector in matters of cybersecurity
Create	Awareness of cybersecurity matters
Provide	Technical support for law enforcement agencies and security agencies to prosecute cyber offenders
Deploy	Strategies to implement research findings towards the promotion of cybersecurity in the country
Establish	And maintain a framework for disseminating information on cybersecurity
Support	Technological advances and research and development in cybersecurity to ensure a resilient and sustainable digital ecosystem
Collaborate	With law enforcement agencies to intercept or disable a digital technology service or product that undermines cybersecurity of the country
Establish	National risk register, register of CII owners, & licensed / accredited persons
Promote	Security of computers and computer systems in the country
Submit	Periodic reports on the state of cybersecurity in the country to the Minister
Establish	Standards for the provision of cybersecurity services
Certify	Cybersecurity products and services
Establish	Codes of practice and standards for cybersecurity and monitor compliance of such by CII owners
Perform	Any other functions which are ancillary to the objects of the Authority

ORGANISATIONAL STRUCTURE

The organisational structure was approved by the Board in consultation with the Public Services Commission.



OVERVIEW OF THE CYBERSECURITY ACT, 2020 (ACT 1038)


Section 35-40
Critical Information Infrastructure
Section 41-46
National and Sectoral CERTs
Section 57-58
Accreditation and Certification
Section 59-61
Cybersecurity Standards, Enforcement and Education
Section 78-80
Realisation of Property
Section 81-82
Industry Forum
Section 83-100
Miscellaneous Provisions

PROFILE OF MEMBERS OF THE GOVERNING BOARD

Hon. Mrs Ursula Owusu-Ekuful (Chairperson)

Mrs. Ursula Owusu-Ekuful is the Minister for Communications and Digitalisation of the Republic of Ghana and the Member of Parliament for Ablekuma West Constituency.

As the Sector Minister, she has oversight of government's infrastructure programmes for the ICT Sector, the development of a robust framework to support the digitisation of the economy and the scaling up of e-government services with a national broadband and total connectivity for the unserved and underserved at the heart of the agenda. She is passionate about supporting the local technology start up ecosystem, nurturing the development of indigenous technology and encouraging women, children and persons with disabilities to engage in ICT.

Mrs. Owusu-Ekuful holds a certificate in Government Integrity from the International Law Institute, Washington DC, a Project Management and Planning Certificate from Ghana Institute of Management and Public Administration and a Masters in Conflict Peace and Security from the Kofi Annan International Peacekeeping Training Centre. She is a lawyer, women's rights activist and a product of the University of Ghana and the Ghana School of Law. She was called to the Ghana Bar in October 1990.

Mrs. Owusu-Ekuful worked for 10 years as an associate at Akufo-Addo, Prempeh & Co. (Legal Practitioners and Notaries Public). From 2005 to 2008, she was the Acting Managing Director of Western Telesystems (Westel) and became the Corporate and External Affairs Director of ZAIN Ghana in the following year.

Dr. Albert Antwi-Boasiako

Dr. Albert Antwi-Boasiako, is the first Director-General of the Cyber Security Authority (CSA). Prior to his appointment, on October 1, 2021, he served as the National Cybersecurity Advisor and Head of the then National Cyber Security Centre (NCSC) from July 2017 to September 2021, leading the institutionalisation of Ghana's cybersecurity development which progressed from 32.6% in 2017 to 86.69% in 2020, according to the ITU's Global Cybersecurity Index (GCI), with Ghana ranked 3rd in Africa and 43rd globally.

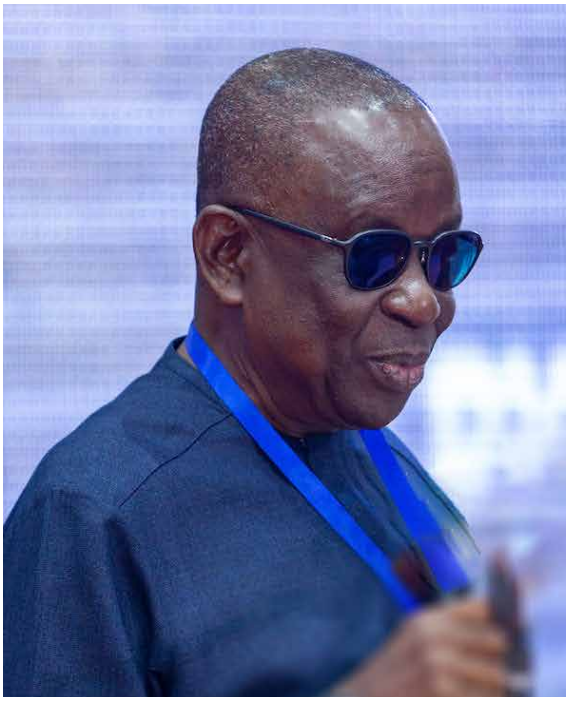
In 2011, Dr. Antwi-Boasiako established e-Crime Bureau, the first cybersecurity and digital forensics firm in West Africa, featuring a state-of-the-art e-Crime Lab. His academic journey includes the successful completion of a PhD at the University of Pretoria in South Africa, where he introduced the Harmonised Model for Digital Evidence Admissibility Assessment (HM-DEAA), contributing significantly to digital forensics standardisation.

Dr. Antwi-Boasiako's educational background includes an undergraduate degree from the University of Trento in Italy, achieved with cum laude honors. He furthered his studies with a postgraduate program at the University of Portsmouth in the United Kingdom, graduating with distinction.

He has conducted cybersecurity related consulting and assignments for international and local organisations including the United Nations Office on Drugs & Crime (UNODC), United Nations Conference on Trade & Development (UNCTAD), the European Union, Commonwealth Cybercrime Initiative (CCI) of the Commonwealth Secretariat, Global Commission on Internet Governance (GCIG)/Royal Institute of International Affairs (Chatham House) and the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA), among others. Since 2014, Dr. Antwi-Boasiako has served as an Expert with the Council of Europe's Global Action on Cybercrime Extended (GLACY+) Project.

He currently serves on the Independent Advisory Committee (IAC) of the Global Internet Forum to Counter Terrorism (GIFCT). He is a Bureau Member of the Cybercrime Convention Committee (T-CY) and is the Government of Ghana's representative on ECOWAS' Regional Technical Committee (RTC) on Cybersecurity. In June 2021, he was recognised as the world's 20th most Influential Security Executive in the Cybersecurity Category by IFSEC Global. He has also received a number of industry awards in Ghana including Top 20 Tech leaders Awards 2022 by the Ghana Information Technology & Telecom Awards and Most Outstanding Personality Award by the Internet Society Ghana Chapter.

He has a number of publications covering information technology, cybersecurity, cybercrimes, data protection and digital forensics to his credit. He has also delivered presentations and papers at major local, regional and international conferences and workshops.



Hon. Albert Kan-Dapaah

Hon. Albert Kan-Dapaah is the Minister for National Security and a Chartered Accountant. He had his first degree from the then University of Professional Studies (UPS), Legon, Accra and continued his accountancy training at the Northeast London Polytechnic and Emile Woolf College of Accountancy.

Hon. Kan-Dapaah worked with Pannel Kerr Forster, a chartered accounting firm, the Social Security and National Insurance Trust (SSNIT) and the Electricity Corporation of Ghana (ECG) and rose from Director of Audit to become Director of Finance, a position he held for six years. He was also a partner at Kwesie, Kan-Dapaah and Baah Co., and a Managing Consultant of Kan-Dapaah and Associates, a utility consultancy support group.

Hon. Kan-Dapaah became a Member of Parliament in 1996, 2000 and 2004 representing Afigya-Sekyere Constituency in the Ashanti Region. He was Minister for Energy in 2000, Minister for Communications and Technology in 2003, and Minister for the Interior in 2004.

Hon. Ambrose Dery

Honourable Ambrose Dery is the Minister for The Interior of Ghana and a Member of Parliament for Nandom in the Upper West Region. He attended the University of Ghana where he graduated with a Bachelor's Degree in Law. He was called to the Bar in 1982 and has since practiced as a Barrister and Solicitor in the Supreme Court of Ghana.

In 2003, Honourable Ambrose Dery was appointed Deputy Attorney-General and further served in two ministerial positions as the Regional Minister for the Upper West Region and Minister of State in the Ministry of Justice.

Honourable Ambrose Dery has been a legislator since 2008 when he won the parliamentary elections to represent Lawra-Nandom Constituency.

Within the period 2009 to 2013, he was the Deputy Minority Leader of Parliament, a Member of the Pan African Parliament, leader of the Pan African Parliament's Observer Mission to the Namibian Presidential and Parliamentary Elections in November 2009, and a leader of the Pan African Parliament fact-finding mission to La Cote d'Ivoire.

Hon. Dominic Nitiwul

Honourable Dominic Nitiwul is the Minister for Defence, Member of Parliament (MP) for the Bimbilla Constituency in the Northern Region of Ghana and served in the Pan-African Parliament since February 2017. He studied Conflict Prevention and Conflict Management at the International Academy for Leadership in Germany, obtained an MBA in Finance from the University of South Wales, and holds a Master of Laws Degree in Corporate Finance from the University of Westminster.

Since 2002, at the age of 25, Honourable Dominic Nitiwul has been the Member of Parliament for the Bimbilla Constituency and was the Deputy Minority Leader of the Ghana's Parliament from 2012 to 2016. He has served on many committees in both the Ghanaian Parliament and the Pan-African Parliament, including Finance Committee, Monetary and Financial Affairs Committee, Business Committee, Appointment Committee, Youth and Sports Committee, Roads and Transport Committee, and Education Committee.

Professor Boateng Onwona-Agyeman

Professor Boateng Onwona-Agyeman is the current Professor & Provost of the College of Basic and Applied Sciences (CBAS) at the University of Ghana, Legon. He obtained a BSc Physics degree from the University of Science and Technology in 1994. He was awarded the Japanese Government Scholarship to study for MSc and PhD degrees in Physics (Experimental Condensed Matter Physics) and Materials science and Engineering respectively from 1997 to 2002.

Professor Boateng was offered a Postdoctoral position with Shizouka National University in Japan from 2005 to 2007. In 2007, he was recruited to join a team of scientists and engineers to develop a porous structure catalyst paper for controlling exhaust gas emissions from small internal combustion engines and for hydrogen production using methane steam reformation. From 2009 to 2012, he worked as Research Associate and Assistant Professor at Kyushu Institute of Technology and Kyushu University respectively in Japan before joining University of Ghana.

Mr. Carl A. Sackey

Mr. Carl Amanor Sackey is a Ghanaian IT expert with over twenty-five (25) years' experience.

Mr. Sackey's working career began with Tara Systems Limited in 1994, where he served as Systems Support Executive, before joining SGS Ghana Limited in 1997, as IT Manager. In 2001 he was appointed Systems Development Manager at the Ghana Community Network Service Limited (GCNet), and he rose through the ranks to become the Deputy General Manager with the role of developing new concepts, products, and architectures and then rolling out these e-solutions for GCNet, the Ghana Revenue Authority, and other stakeholders such as the Bank of Ghana.

He was a member of the committee that developed some of the IT Governance documents for the Ministry of Communications Digitilisation and was a member of the then National Cyber Security Technical Working Group.

Mr. Amanor Sackey is a Computer Science Graduate of the University of Science and Technology, now KNUST and holds an MBA from the China Europe International Business School (CEIBS).
He lectures in IT Security, Audit, Risk, Cyber Security and Governance in many institutions and has served two terms as President of ISACA Accra Chapter, a global professional body for IT Auditors, Risk, Governance and Information Security Professionals.

Mr. Reginald Botchwey

Mr. Reginald Botchwey is the CEO and Co-Owner of Global Link Services, a technology consulting and staffing company

He holds a Bachelors Degree in Computer Science and a Masters Degree in Software Engineering from the University of North Carolina Charlotte.

Mr. Botchwey has 26 years of experience in both public and private sectors specialising in software engineering and big data solutions architecture across the financial, engineering and risk sectors.

Mrs. Adelaide Benneh-Prempeh

Mrs. Adelaide Benneh-Prempeh is a seasoned corporate lawyer and founder/managing partner at B&P associates. She is a top ranked lawyer in the Corporate/Commercial Chambers & Partners Global Guide whose expertise spans across sectors. Her focus practice areas include Energy, Mining and Power, Construction and Infrastructure, Project Finance and Development, and Commercial transactions. The rest are Employment and labour, Corporate Governance and Compliance, Restructuring and Insolvency, among others.

Mrs. Benneh-Prempeh is a certified Insolvency Practitioner and Insolvency Consultant to the International Finance Corporation (IFC) of the World Bank Group on the Ghana Investment Advisory Project. She began her legal career with the law firm Lovells (now Hogan Lovells) in London, and later joined Renaissance Chambers, also in London. She is currently a senior practitioner with Bentsi-Enchill Letsa & Ankomah in Accra, Ghana. She is also an Advocacy and Ethics lecturer at the Ghana School of Law and a Notary Public.

Mrs. Mavis Vijaya Afakor Amoa

Mrs. Mavis Vijaya Afakor Amoa is a Barrister and Solicitor of thirty-three years standing, a Notary Public and Legislative Drafter. She holds an Advanced Diploma in Legislative Drafting obtained in 1992 from the University of West Indies and an Executive MBA obtained in 2008 from the Ghana Institute of Management and Public Administration.

She has served as the Director for Legislative Drafting from 2016 to date. She has over 29 years of legislative drafting experience, as drafting counsel with the Office of Attorney-General and Ministry of Justice in Ghana.

Her drafting experience covers a wide range of primary and secondary legislation including subject areas such as energy, companies, public financial management, environmental law, maritime security law, anti-money laundering, insurance, cybersecurity and implementation of treaties.

Mavis also lectured in Legislative Drafting in respect of a training programme organised in Ghana under the auspices of the Commonwealth Secretariat and the Ghana School of Law in Ghana.

Mavis has worked in collaboration with experts from the Commonwealth Secretariat, international consultants, the IFC and World Bank on a number of drafting assignments.

Mavis is a member of the Ghana Bar Association and the Commonwealth Association of Legislative Counsel.

Mrs. Esther Dzifa Ofori

Mrs. Esther Dzifa Ofori is a Ghanaian diplomat and marketing expert. After reading English at the University of Ghana, Legon, Mrs. Ofori worked at the Ghana Tourist Development Board and Social Security Bank (SSB), now Société Générale where she worked for 15 years as the Public Relations Manager. Mrs. Esther Dzifa Ofori also worked with Multichoice Ghana as the Commercial Manager.

On leaving Multichoice, Mrs. Ofori set up a consultancy specialising in Management and Public Relations before being appointed as the Chief Executive of the Ghana Trade Fair Company.

Her role at the Trade Fair was not only to manage the huge Estate Complex on a commercial basis but also to use the medium of the numerous fairs, to promote local goods and services as well as foreign imported goods. She was trained in public relations, executive communications skills and human resource development.

From 2017 to 2020, Mrs Ofori was appointed as Ghana's Ambassador to Equatorial Guinea where she strengthened the relationship between Ghana and Equatorial Guinea. She developed and facilitated an educational exchange program for the people of Equatorial Guinea to study English in Ghana rather than in Nigeria and England.

Through the years, she has been a Television Presenter for Women's Digest -Women's Magazine Programme, Toddlers Time - Children's Programme and Good Cooking with Maggie – a Unilever Cooking Show.

CSA SENIOR MANAGEMENT TEAM

- Dr. Albert Antwi-Boasiako
  Director-General
- Mercy Araba Kertson
  Head, Administration
- Alexander Oppong
  Head, Capacity Building and Awareness Creation
- Benjamin Ofori
  Head, Critical Information Infrastructure Protection
- Emmanuel Agah
  Head, Law Enforcement and Liaison Unit
- Johnson Awua
  Head, Finance
- Ebenezer Osei-Kofi
  Head, Internal Audit
- Efua Brown-Eyeson
  Head, Child Online Protection

REPORT

By Chairperson of the Governing Board

Introduction

Following the inauguration of the maiden Board of the Cyber Security Authority (CSA) on February 18, 2022, it is a pleasure to present the first Annual Report of the Authority for the year ended 2022 as part of the legal obligations under section 28 of the Cybersecurity Act, 2020 (Act 1038).

The inauguration of the Governing Board of the Authority was a major milestone in 2022 as it sets the pace for the Authority to fully operationalise its mandate as stipulated in the Cybersecurity Act, 2020 (Act 1038).

Cybersecurity Regulations

As a regulator in the cybersecurity space, it was necessary to put in place the necessary modalities for the regulations of the cybersecurity activities in Ghana and for the protection of Critical information infrastructure. In consultation with relevant stakeholders, the Authority put in place relevant structures to kick start its regulatory regime in 2023.

To effectively regulate the industry and operationalise its mandate, human resource was identified as one of the most important areas of focus for the Authority and this led to the development and approval of an Organisational Manual and Schemes of Service to support the recruitment and retention of competent staff.

To further ensure a clear-cut direction on cybersecurity matters for the Authority and the country at large, the National Cybersecurity Policy and Strategy was given a final review and subsequently approved by the Board, pending cabinet's endorsement.

In furtherance to the appointment of members of the Joint Cybersecurity Committee, the Committee was inaugurated to ensure the implementation of cybersecurity measures per section 13 and 14 of the Cybersecurity Act.

Outlook for 2023

In 2023, the Authority will start the implementation of its regulatory regime to ensure the licensing of Cybersecurity Service Providers, the accreditation of Cybersecurity Professionals and the accreditation of Cybersecurity Establishments, among other regulatory interventions.

We will also improve our stakeholder engagements and see to the establishment of the Industry Forum pursuant to section 81 of the Act.

Acknowledgement

The year under review saw the right foundations being laid for this very new and yet critical institution as far as the digitalisation efforts and the socio-economic development of our country is concerned. I am therefore thankful to the Board, Management and Staff of the Authority for their resilience and diligence this past year.

We appreciate the support of the President of the Republic, H.E. Nana Addo Dankwa Akufo-Addo and his Vice, H.E. Alhaji Dr. Mahamudu Bawumia.

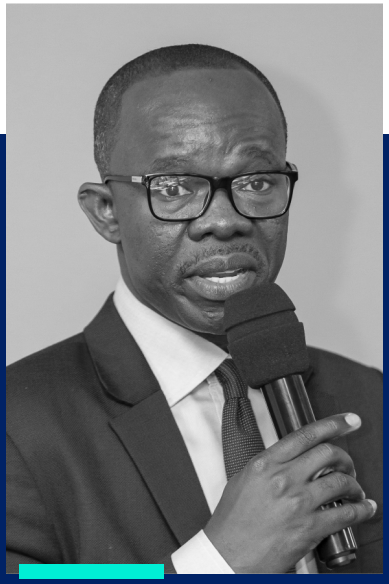
Further appreciation goes to the Ministries of Communication and Digitalisation, National Security, Defence and The Interior for the effective collaboration over the year.

We are grateful to all stakeholders for engaging with us and keeping us on our toes to deliver on our mandate.

Hon. Mrs. Ursula Owusu-Ekuful
Chairperson, CSA Governing Board
December, 2022

REPORT

By Director-General



Background

The Cyber Security Authority (CSA) was established on October 1, 2021. As a start-up institution, a lot of attention has been on putting in place relevant structures to ensure the foundation is solid to build a world-class cybersecurity institution for a secure and resilient digital ecosystem. There have been challenges and opportunities but with the support of the Governing Board, the management team and staff, we have been able to take some very bold decisions with respect to staffing, financing, and especially with respect to operationalising the mandate of the Authority as prescribed by the Cybersecurity Act, 2020 (Act 1038).

Regulatory Interventions

In 2022 following the direction of the Governing Board, we commenced a number of regulatory processes including initiatives that would ensure the protection of Critical Information Infrastructures, pursuant to Sections 35 to 40 of Act 1038; licensing of Cybersecurity Service Providers pursuant to Sections of 49 to 56 and regulations on operations of Computer Emergency Response Teams, cybersecurity incident reporting and response, pursuant to Sections 41 to 48 of the Cybersecurity Act, 2020.

The implementation of these cybersecurity regulations is imperative to deal with both existing and emerging cyber threats that have the potential to undermine the digital dividends expected from our digital economy.

Critical Information Infrastructure Registration

Sections 35-40 of Act 1038 provide for the designation of computer systems or computer networks as Critical Information Infrastructure (CII). Consequently, a total of 13 sectors had been designated in 2021 as CII, pursuant to Gazette No. 132 published on Thursday, September 23, 2022. In 2022, the Authority commenced registration procedures and requirements pursuant to the implementation of Section 36 of the Cybersecurity Act, 2020 (Act 1038) and has since developed a Database for CII Points of Contact. The Authority has also commenced the process of registering all CII Owners and their systems.

Finance and Administration

The Authority is grateful to the Ministry of Communications and Digitalisation, the National Communications Authority and other partners for the financial and logistical support over the years that has positioned the Authority to run its operations. As part of efforts to become financially stable as an institution, the CSA has engaged the Ministry of Finance in the identification and development of Internally Generated Funds (IGF) sources pursuant to Section 23 of Act 1038.

The Authority ended the year with a total of 84 employees; 47 males and 37 females. Amongst these were 3 officials seconded from other state institutions to support the Authority with the implementation of its mandate.

Incident Reporting Points of Contact (PoC)

The Cybercrime/Cybersecurity Incident Reporting Points of Contact (PoC) was launched in October 2019. From January to December 2022 alone, a total of 9,123 contacts were made with the CSA through the PoC. 628 of the contacts were actual cyber-related incidents, and a total of 8,485 represents those who reached out to the National CERT of the CSA for guidance and advisories to prevent cybercrime incidents (i.e., government institutions, businesses, the public and children).

International Cooperation

International cooperation is critical to cybersecurity development due to the borderless nature of cybercrimes. With Ghana being identified as a hub for training and capacity building for the sub region by the European Commission, Council of Europe (COE), World Bank, ECOWAS, among others, the country, through the CSA, has hosted several international capacity-building programmes and also contributed to international cooperation efforts through knowledge and experience sharing on international platforms like the World Bank, World Economic Forum, Global Cybersecurity Forum, among others. Ghana has signed Memoranda of Understanding (MoUs) with Rwanda and Mozambique to further strengthen collaborative and capacity-building efforts and further held bilateral meetings with Singapore, Saudi Arabia and the World Economic Forum. The CSA has also engaged foreign missions in Ghana like the USA, Czech Republic, Italy, UK, Canada, etc on ways to collaborate with respect to capacity building in cybersecurity matters.

Child Online Protection

The Cyber Security Authority, as a regulator, is committed to ensuring the protection of children online per its mandate in sections 62-66 of the Cybersecurity Act 2020. The National Child Online Protection (COP) Framework, which was developed in 2016, has been revised to incorporate the new Cybersecurity Act, 2020 (Act 1038), the 2020 ITU COP Guidelines and the WePROTECT Model National Response (MNR) Framework, an international framework for COP response. The Authority's efforts and commitment to COP issues and cybersecurity development, in general, was commended in a Daily Graphic Editorial of September 20, 2022, with the heading "Digitally safe country necessary".

Stakeholder engagements

Cybersecurity is multisectoral in nature and collaboration with relevant stakeholders plays a significant role in ensuring the CSA executes its mandate successfully. It is for this reason that the Authority was committed to the establishment of the Joint Cybersecurity Committee (JCC), in July 2022 in accordance with sections 13 and 14 of Act 1038, for the implementation of effective cybersecurity measures. Plans are also advanced for the establishment of the Industry Forum pursuant to section 81 of Act 1038 for enhanced collaboration with the private sector and all industry players on cybersecurity matters in 2023.

Capacity Building and Awareness Creation

Cybersecurity consciousness and good cyber hygiene practices are critical to solving over 90% of cybercrimes and cybersecurity-related issues. As part of efforts to champion the creation of a cybersecurity culture among the Ghanaian population, the CSA in 2022 engaged several institutions including religious bodies to build capacity and to create awareness on cybersecurity matters. The annual National Cyber Security Awareness Month (NCSAM) was further successfully organised on the theme: "Regulating Cybersecurity; A Public-Private Sector Collaborative Approach." The month-long event brought different stakeholders together to discuss the way forward for Ghana's cybersecurity development.

The way forward

Ghana has already made admirable strides in its cybersecurity development and is already a model for many countries in Africa and beyond. The future of cybersecurity development is a desire to see Ghana's cybersecurity infrastructure as one of the best in the world and its overall cybersecurity development named first in Africa and among the top 25 globally.

In furtherance to the government's agenda to ensure a fully digitalised economy, the Cyber Security Authority is poised to ensure that government digitalisation efforts are sustained, and critical information infrastructure is protected. 2023 will be a very busy year for the Authority as it commences its regulatory regime by licencing and accrediting cybersecurity service providers, cybersecurity establishments and cybersecurity professional.

Furthermore, as the country continues to digitise, there will be a conscious effort to develop cybersecurity expertise to serve the national need. The Authority will also continue to use various awareness creation and capacity building modules to develop a cybersecurity culture in all sectors of the country. CSA will continue to explore opportunities in cybersecurity and put in place the necessary measures needed to ensure a safe online experience for all Ghanaians.

Appreciation

I am honoured to lead this young institution that promises to be a world-class cybersecurity institution in the very near future. On behalf of the Board and Management, I wish to thank all staff and stakeholders for their continued efforts and support. I thank the members of the JCC for their collaboration and I look forward to working together with all stakeholders for a secure and resilient digital Ghana.

Dr. Albert Antwi-Boasiako
Director-General, (CSA)

CORPORATE GOVERNANCE

Governing Body

In accordance with Section 5 of the Cybersecurity Act, 2020 (Act 1038), the Authority is governed by a Governing body which was inaugurated in February 2022.

Pursuant to section 5(1) of Act 1038, the composition of the Governing Board consists of:

- the Ministers responsible for
  - Communications;
  - the Interior;
  - National Security; and
  - Defence;
- the Director-General of the Authority;
- three persons from the Industry Forum nominated by the Industry Forum; and
- three other persons nominated by the President on the advice of the Minister, at least two of whom are women.
- Section 5(2) of the Act indicates that the President shall nominate the Minister as chairperson of the Board. Section 5(3) further provides that the chairperson and other members of the Board shall be appointed by the President in accordance with article 70 of the Constitution.

Meetings of the Board

Pursuant to section 8(1) of the Cybersecurity Act 2020 (Act 1038), the Board is expected to meet at least once every quarter for the conduct of business at a time and place determined by the chairperson.
According to section 8(2), the chairperson requests in writing of not less than one-third of the membership of the Board, to convene extraordinary meetings of the Board at a time and place determined by the chairperson. As indicated in section 8(3) of the Act, the chairperson presides at meetings of the Board and in the absence of the chairperson, a member of the Board, other than the Director-General, is elected by the members present from among their number to preside.
Pursuant to section 8(4) of Act 1038, a quorum is formed at a meeting of the Board when there are seven members of the Board present. Matters before the Board are decided by the majority of the members present and voting, in the event of an equality of votes, the person presiding has a casting vote.

Board Sub-Committees

Pursuant to section 10(1) of Act 1038, the Board has established committees consisting of members of the Board and non-members or both, to perform the functions of the Board. Section 10(2) provides for the committees to be composed of members and non-members and shall be chaired by a member of the Board. According to Section 10(3) non-Board members on a committee of the Board are only advisory members. The established committees are:

- Finance and Administration
- Technical

Major Decisions Made or Resolutions Passed by the Board

The following major decisions/resolutions were made or passed by the Board during the year under review:

- Approval of the National Child Online Protection Framework
- Approval of the National Cybersecurity Policy and Strategy
- Approval of Licensing of Cybersecurity Service Providers and Accreditation of Cybersecurity Professionals and Cybersecurity Establishments
- Approval of Regularisation of Staff of the Cyber Security Authority

Disclosure of interest

Section 9(1) of Act 1038 provides that a member of the Board who has an interest in a matter for consideration by the Board should disclose in writing the nature of that interest and the disclosure shall form part of the records of the consideration of the matter; and the member is disqualified from being present at or participating in the deliberations of the Board in respect of that matter.
No member of the Board declared interest in any matter considered by the Board during the year 2022.

Board Members' allowances

Members of the Board and members of a committee of the Board are paid allowances determined by the Minister in consultation with the Minister responsible for Finance.

MANDATE OF FUNCTIONAL AREAS

National CERT (CERT-GH)

Pursuant to Sections 41 to 46 of Act 1038, the National Computer Emergency Response Team (CERT-GH) is responsible for receiving, analysing and responding to cybersecurity incidents; co-ordinating responses to cybersecurity incidents among public and private institutions, and international bodies such as Forum of Incident Response Security Teams (FIRST); overseeing the operations of Sectoral CERTs; operationalising the 24/7 Cybercrime/Cybersecurity Incident Reporting Points of Contact (PoC); threat intelligence gathering and analysis, and the issuance of alerts and advisories on potential, imminent or actual cyber threats, vulnerabilities or incidents affecting Ghana's cyber ecosystem.

Critical Information Infrastructure Protection (CIIP)

Pursuant to Sections 35 to 40 of Act 1038, the Critical Information Infrastructure (CII) Protection functional area is responsible for protecting all critical systems that sustain Ghana's digital economy; developing and operationalising a Risk Management Framework for CIIs and Government Digitalisation Initiatives (GDIs); coordinating crisis management and the response of all CII related incidents; carrying out compliance monitoring of CII in adherence to the CII Directive, and acting as a point of contact between CIIs and the CSA on all CII engagements.

Capacity Building & Awareness Creation (CBAC)

Pursuant to Sections 60 of Act 1038, the Capacity Building and Awareness Creation (CBAC) functional area is responsible for raising awareness and building capacity on cybercrime and cybersecurity-related issues among Children, the Public, Businesses, and Government; leading the implementation of the Safer Digital Ghana programme; developing programmes and events for cybersecurity education and capacity building; overseeing cybersecurity skills development and training programmes for the public sector in particular.

Child Online Protection (COP)

Pursuant to Section 4(j) of Act 1038, the CSA through the COP functional area in implementing the COP provisions of the Act is responsible for overseeing policy development, capacity building, and awareness creation on COP-related issues in collaboration with stakeholders; - such as Ministry of Education, Ministry of Gender, Children and Social Protection, Plan International and the UNICEF;

- Development of the draft National COP Framework to protect the activities of children on the internet.
- Operationalising and supporting the COP technology system.
- Supporting and coordinating the prosecution of Child Online offences and providing legal support to victims.
- Acting as a point of contact between the CSA and COP stakeholders.

Law Enforcement Liaison Unit (LELU)

Pursuant to Sections 69 to 77 of Act 1038, the Law Enforcement Liaison Unit (LELU) is responsible for coordinating law enforcement related functions of the CSA. These functions include assessing cases, identifying leads and coordinating investigations of specific cybersecurity incidents; engaging with the Office of the Attorney-General on prosecution of cases, implementing the substantive provisions under Sections 69-77 of Act 1038; coordinating engagements with law enforcement and security agencies on cybersecurity and investigatory powers; providing critical advice and guidance to relevant agencies on how to use the investigatory powers to facilitate investigations and prosecution of cybercrime cases and implementing the data retention and preservation mandates in Act 1038. LELU also serves as the 24/7 point of contact based on Article 35 of the Budapest Convention on cybercrime.

Legal & Compliance (LECO)

The Legal and Compliance functional area is responsible for providing legal advice and support to the CSA and overseeing the legal functions of the Authority. Pursuant to Sections 49 to 59 of Act 1038, LECO is further mandated to provide regulatory guidance and directions relating to Compliance & Enforcement, Licensing,

Cybersecurity Professionals, and the maintenance of a licence/accreditation registry. The functional area has a mandate to support the CSA to develop regulatory policies, guidelines, and directives in accordance with Sections 59, 91 and 92 of Act 1038.

Cybersecurity Technology Standards

Pursuant to Sections 71 to 76 of Act 1038, the Cybersecurity Technology Standards (CTS) functional area is responsible for developing and promoting data interception capabilities and retention standards for service providers; providing guidance on lawful interception capability specification for service providers; providing guidance on data preservation by regulated service providers pursuant to Section 77 of Act 1038; developing and implementing technology standards for cybersecurity; conducting testing and assurance in compliance with cybersecurity standards pursuant to Section 59 of Act 1038, and providing advisories/standards for cybersecurity products and services.

Information Technology (IT) Services

The Information Technology (IT) Services functional area is responsible for designing and implementing the technology infrastructure of the CSA; deploying and managing applications and services to enhance operational IT needs and requirements of the CSA and adopting policies and standards to govern the implementation of IT Services.

Joint Cybersecurity Committee (JCC) Secretariat

Pursuant to Sections 13 and 81 of Act 1038, the Joint Cybersecurity Committee (JCC) Secretariat is responsible for coordinating the work of the JCC and the Industry Forum respectively, in the implementation of Act 1038. This function includes engaging with the institutions represented on the JCC for the implementation of relevant cybersecurity measures and providing assistance to the Industry Forum in the development and implementation of the Industry Code as provided in Section 82 of Act 1038.

Administration

The Administration functional area is responsible for the day-to-day administrative operations and management of the Cyber Security Authority (CSA). This functional area has a central role of providing administration support services to the various functional areas and supporting the Director-General in the day-to-day administration of the CSA. The Administration functional area provides administrative support services, including transport, estate, and security for the CSA. The functional area also plays an oversight responsibility for Human Resource Administration and Procurement-related matters. In addition, the functional area also plays an oversight role on International Cooperation by supporting the efforts of the CSA to secure the cyberspace through international collaborations in line with section 83 of the Cyber Security Act.

Finance

Pursuant to Sections 23 to 25 of Act 1038, the Finance functional area is responsible for the general financial management of the CSA by providing general oversight over accounts related matters subject to the Public Financial Management Act, 2016, (Act 921); spearheading the establishment and management of the Cybersecurity Fund pursuant to Section 29 of Act 1038; managing the general financial resources, assets, and properties of the Authority; generating regular periodic/annual and other financial reports of the Authority and performing all the financial-related functions of the Authority as prescribed by Act 1038.

Internal Audit

Pursuant to Section 22 of Act 1038 and in compliance with Section 83 of the Public Financial Management Act, 2016 (Act 921), the Internal Audit functional area is responsible for generating regular audit reports of the CSA for the Governing Board, the Director-General, and the Internal Audit Agency in accordance with Section 16(3) & (4) of the Internal Audit Agency Act, 2003 (Act 658) and other internal audit-related functions of the CSA.

Communications

The Communications Unit is responsible for internal and external communication & corporate affairs related activities of the Authority. The Unit works closely with all other functional areas to promote the activities of the CSA.

ADMINISTRATION

Human Resources

Workforce Planning, Staff Turnover and Retention

The Authority in 2022 ensured that the management of its Human Resources aligned with its mandate and vision and developed a workforce plan to support current and future human resource needs. To improve manpower capacity, the CSA secured financial clearance from the Ministry of Finance to undertake a regularisation exercise to provide permanent employment for staff. In addition, the CSA with the support of other public sector organisations, received seconded officers to augment the staffing capacity in achieving its mandates.

Staff Compensation

During the period, majority of the staff of the Authority, with the exception of those on secondment, were engaged on contract. Management however ensured that their compensations were competitive and regular to make them relatively comfortable.

Statistics On Staffing

The Authority had a total staff strength of eigthy-four (84), with forty-seven (47) staff members representing 56% being males, and thirty-seven (37) staff members representing 44% being females. The total strength included three (3) seconded staff from other public service institutions joining the CSA to achieve the mandate.

Category	Male	Female	Total
Management	6	2	8
General	41	35	76
Total	47	37	84
Percentage Gender Ratio	56%	44%	100%

During the year, a total of five (5) officials left the Authority. These separations were largely due to new opportunities or to further their education.

Shift & Flexible Working System

To effectively deliver the core mandate of the CSA, especially in the area of incidence reporting and response, the Authority implemented a shift and flexible working system in 2022. This was to ensure that staff from the related functional areas (especially the CERT-GH and the CIIP team) operate a shift system to provide 24-hour services to the CERT ecosystem, all designated CIIs and other critical cybersecurity needs of the country. This arrangement also allowed for the remote working of other officials who could produce verifiable and measurable outputs or results whilst working from home.

Professional Development

The CSA believes that investing in the professional development of employees is essential to the success of the Authority. In 2022, the Authority offered a variety of training and development programmes, including in-house training and certification programmes like the Certified Security Principles+ (CSP+) which was compulsory for all staff.
The Authority also provided support for employees who wanted to pursue higher education through flexible work arrangements.

Development and Implementation of Leave Management Policy

An Annual leave Policy was developed and implemented to ensure the promotion of a healthy and productive workforce.

Enforcement and Disciplinary Policy

To outline measures for ensuring adherence to and enforcement of the core values and practices of the CSA, the Authority developed an Enforcement and Disciplinary Policy which took effect from March 2022.

Performance Appraisal System

To evaluate employee performance during the year, an appraisal system was instituted to evaluate employee performance in line with the CSA's goals and objectives.

Development of Schemes of Service, Organisational Manual and Conditions of Service

As part of requirements to fully operationalise a public sector institution such as the Cyber Security Authority (CSA), the CSA developed an Organisational Manual, Schemes of Service and Conditions of Service in collaboration with the Fair Wages and Salaries Commission and the Public Services Commission.

Quarterly staff meeting

Employees are kept informed about the affairs of the Authority and provided with the opportunity to express their opinion on key management decisions through these quarterly staff engagements.

Procurement and purchasing

Procurement transaction for 2021/2022

Procurement by Method

Method	No. of Contract Issued	Percentage Per Value
Restrictive Tendering Procedure (RTP)	10	19.6%
Shopping/RFQ	41	80.4%
Total	51	100%

Procurement by Method

Category	No. of Contract Issued	Percentage Per Value
Goods	30	57.7%
Services	22	42.3%
Total	52	100%

Establishment of the Entity Tender Committee (ETC) as per Section 21 (3) of the Public Procurement Act 663

The Authority on April 29, 2022, inaugurated the Entity Tender Committee (ETC) as per the Public Procurement Law, 2003 (Act 633)/ Act 914 (2016) to review and approve annual procurement plans and quarterly updates of procurement plans to ensure that they support the objectives and operations of the Authority.

Procurement Status Approval

During the year, the Authority gained Procurement Status Approval from the Public Procurement Authority.

Risk Management Responsibilities

Board

The Finance and Management Sub-Committees of the Board is responsible for overall risk management in the Authority.

Management

The sub-committee manages risks as part of their operational responsibility to identify, assess and control risks that may affect the Authority.

Internal Audit

The Internal Audit functional area of the Authority plays a pivotal role in assisting Management in the control of risks. It reports to the Board through the Finance and Management Sub-Committees.

OVERVIEW OF OPERATIONAL PERFORMANCE

Strategic Objectives

In line with the Authority's core mandate as prescribed by the Cybersecurity Act 2020 (Act 1038), the Authority's operations in 2022 were guided by goals determined by the Board and Management decisions. Accordingly, Divisions set goals and objectives to guide their day-to-day operations.

Inauguration of the Governing Board

As part of the process to effectively implement the Cybersecurity Act, 2020 (Act 1038), the Governing Board of the Authority was inaugurated on Friday, February 18, 2022, pursuant to Section 5 of the Act 1038. The Governing Board has been established to provide oversight responsibility for the Authority and to provide policy and strategic direction for the effective performance of the functions of the Authority.

Inauguration of the Joint Cybersecurity Committee (JCC)

Pursuant to Section 13 of the Cybersecurity Act, 2020 (Act 1038), a Joint Cybersecurity Committee (JCC) consisting of heads of eighteen (18) public sector institutions with a mandate on cybercrime/cybersecurity matters was established and inaugurated on Thursday, July 14, 2022. The JCC, in accordance with Section 14 of the Act, is to collaborate with the Authority and the sectors or institutions represented on the Committee for the implementation of relevant cybersecurity measures. The Committee is answerable to the Governing Board in the performance of its functions.

Consultative meetings on the implementation of Act 1038

The CSA in 2022 held consultative meetings with key stakeholder institutions to improve upon existing areas of collaboration and to further identify new areas of collaboration. Among the institutions are the Bank of Ghana (BoG), National Communications Authority (NCA), National Information Technology Agency (NITA), the Ghana Association of Banks (GAB) and the Narcotics Control Commission (NCC). The engagements concluded with joint statements and are being followed up with Memorandum of Understanding.

Development of Framework for the Licensing of Cybersecurity Service Providers, Accreditation of Cybersecurity Establishments and Accreditation of Cybersecurity Professionals

Pursuant to Sections 4(k), 49, 57 and 59 of the Cybersecurity Act, 2020 (Act 1038) which mandates the CSA to regulate cybersecurity activities including the licensing of cybersecurity service providers (CSPs), accreditation of cybersecurity establishments (CEs) and accreditation of cybersecurity professionals (CPs); the CSA has developed a draft Framework for the licensing of CSPs; accreditation of CEs and accreditation of CPs aimed at ensuring that CSPs, CEs and CPs attain a higher level of compliance with Act 1038 and standards in line with international best practices. The Framework, which has received inputs from relevant stakeholders, is to guide the implementation of the licensing and accreditation regimes for CSPs, CEs and CPs which is scheduled to start in 2023.

Development of Framework for the Accreditation of Sectoral Computer Emergency Response Teams (CERTs)

Pursuant to Section 44(4) of the Cybersecurity Act, 2020 (Act 1038) which mandates the CSA to accredit and oversee the operations of Sectoral CERTs, the CSA has developed a draft framework for the accreditation of Sectoral CERTs to ensure oversight supervision of the operations of the Sectoral CERTs and compliance with incident reporting obligations across the various sectors. The Accreditation framework is expected to be considered by the Governing Board for implementation, starting January 2023.

Registration of Critical Information Infrastructure (CII)

Following the publication of Gazette Notice No. 132 in September 2021, a total of 13 sectors of the country were identified and designated by the Minister for Communications and Digitalisation as Critical Information Infrastructure (CII) Sectors. The registration of these identified CIIs therefore started in 2022 pursuant to Section 36 of Act 1038 and Gazette Notice No. 140. The CII registration process involves 4 major milestones:

- Nomination of CII Point of Contact
- Capacity building workshops on the CII Registration Process,
- Submission of details of critical systems
- Issuance of the Certificate of registration

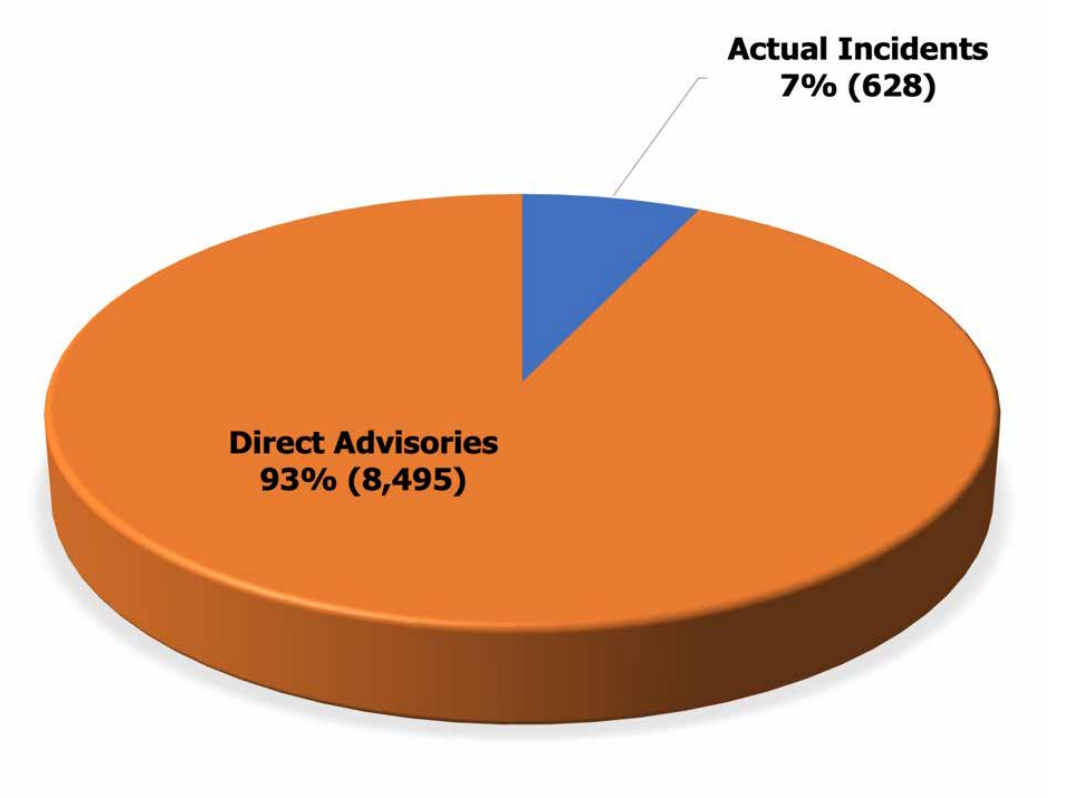
Milestones for CII Registration	Current Update
Nomination of CII Point of Contact	90% of CII Owners have nominated their CII Points of Contact.
Capacity Building Workshops on the CII Registration Process	83% of CII Owners were trained on the CII Registration Process through the capacity building workshops
Submission of details of critical systems	21% of CII Owners have submitted the details of their critical systems to the CSA

The designation and registration of CII is to give full effect to Sections 35 – 40 of Act 1038 for the protection of all critical information sectors of the country's economy in view of the current digital transformation agenda.

Performance of the Cybercrime/Cybersecurity Incident Reporting Points of Contact (PoC)

From January to December 2022, a total of 9,123 contacts have been made with the CSA through the PoC. 628 of the contacts were actual cyber related incidents.

Total Contacts Made Through The POC - 9,123

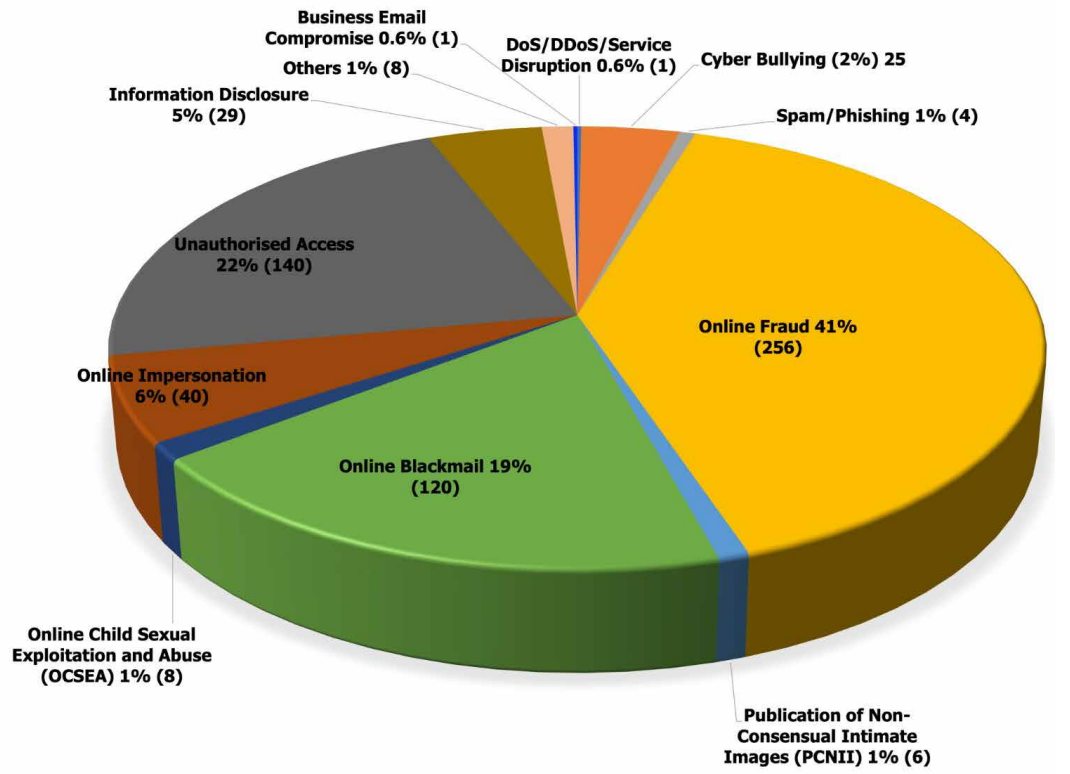


8,485 direct advisories were issued through the PoC to various government institutions, businesses, the public and children covering how to protect online accounts (bank, email, social media) from being compromised by enabling two-factor authentication, creating strong passwords, how to detect common online fraudulent schemes etc. These advisories have equipped constituents to avoid becoming potential victims of cybercrime.

The 628 actual incidents are categorised into:

- Online Fraud (Investment scam, online shopping fraud, job recruitment fraud, etc)
- Unauthorised Access (WhatsApp account takeover, Phishing etc)
- Online Impersonation
- Online Blackmail (Sextortion)
- Publication of Non-consensual Intimate Images
- Cyber Bullying
- Online Child Sexual Exploitation and Abuse
- Spam/Phishing
- Information Disclosure
- DDoS/Service Disruption and
- Business Email Compromise

Top Reported Incidents at the PoC



Sponsorship of GCB Security Operations Centre (SOC) application for FIRST Membership

The Forum for Incident Response and Security Teams (FIRST) facilitates information-sharing, incident response and prevention, vulnerability analysis, computer security, management and policy issues, and research towards the prevention of cyber-attacks on worldwide platforms and systems. It was established in 1990 and currently boasts of a membership of 575 teams comprising government bodies, universities, corporations, and other institutions across several countries.

CERT-GH became a member of FIRST in June 2021 and in line with the CSA's mandate to collaborate with international agencies to promote the cybersecurity of Ghana, CERT-GH sponsored the GCB Bank SOC as part of the requirements for them to become members of FIRST. The process was successfully completed in November 2022; making GCB Bank the first Ghanaian organisation after the CERT-GH to achieve this.

Capacity Building and Awareness Creation

The Authority organised several awareness creation and capacity building programmes in academic institutions, religious institutions and among development partners and Civil Society Organisations.

National Cyber Security Awareness Month (NCSAM) 2022

The National Cyber Security Awareness Month (NCSAM) is a flagship initiative under the five-year National Cybersecurity Awareness Programme dubbed **A Safer Digital Ghana** with a focus on Children, the Public, Businesses and Government.

The 2022 edition of NCSAM was organised under the theme **"Regulating Cybersecurity: A Public-Private Sector Collaborative Approach".** The event aimed at engaging with relevant stakeholders to deliberate on the Act and its implications, as Ghana seeks to build upon its foundational cybersecurity pillars. The month-long event focused on key areas of Ghana's cybersecurity development.
The following are some of the activities and programmes organised during the month-long event:

- Official Launch of NCSAM 2022 and the signing of the Memorandum of Understanding (MoU) between the CSA and the National Information and Communications Technology Institute (INTIC) of Mozambique and the National Cyber Security Authority (NCSA) of Rwanda.
- Public Consultation on Framework for the Licensing of Cybersecurity Service Providers, Accreditation of Cybersecurity Establishments and Accreditation of Cybersecurity Professionals.
- Forum on Ghana's Cybersecurity Regulations and Opportunities for Cybersecurity Industry Players and Professionals.
- Public Consultation on Framework for the Accreditation of Sectoral CERTs.
- Compliance Workshop on the Directive for the Protection of Critical Information Infrastructure (CII).
- Civil Society Forum on Regulating Cybersecurity through Strategic Partnership.
- Cyber Security Authority/Ghana Association of Banks Bank Boards and Executive Directors Briefing on "Ghana's Cybersecurity Act, 2020 (Act 1038); the Bank of Ghana Cyber and Information Security Directive; Its Implications and the Roles of Board of Directors".
- There were also a number of activities with institutions like the Chamber of Telecommunications, groups and associations, and the media among others.

Capacity Building Activities

A number of Awareness Creation and Capacity Building programmes were organised by the Authority in collaboration with local and international partners as follows:

- CSA coordinated the organisation of the maiden African Union (AU) Global Forum for Cyber Experts (ACE) Meeting from March 16 to 18, 2022, in Accra, Ghana.
- A workshop on Advisory Mission on Search, Seizure, and Confiscation of Online Crime Proceeds was organised for law enforcement agents and other members of the criminal justice sector in Accra from May 30 to June 01, 2022.
- The Authority represented the Ministry of Communications and Digitalisation to host the Global Internet Forum to Counter Terrorism (GIFCT) Workshop on Countering Terrorism and Violent Extremism Online in September 2022.
- E-Evidence First Responder Trainer Course (EFR-TOT) spanning from June to July, 2022 was organised for law enforcement agents.
- Introductory Training Course on Cybercrime for Judges and Prosecutors and training of trainers Part I, was hosted in Accra from December 6 to 9, 2022.

Organisations (CSOs) may help with the effective implementation of the Cybersecurity Act, 2020 (Act 1038) organised by the Media Foundation for West Africa (MFWA) in Accra.

- Participation in the Girls in ICT mentorship programme organised by the Ministry of Communications and Digitalisation.
- Awareness Creation and Capacity Building Training for Teacher Mentors of Campaign for Female Education (CAMFED)on March 11, 2022.
- Cybersecurity sensitisation exercises for religious groups in the country.
- Lecture Series in selected tertiary institutions across the country.
- Webinars on cybersecurity-related matters for different associations and groups.

Statistics on key capacity building and awareness creation events

S/N	Events	Audience Reached
1	Kick-Off Meeting on the African Union (AU) Global Forum for Cyber Experts (GFCE); coordinated the organisation of the African Community Experts (ACE) from March 16 to 18, 2022, in Accra, Ghana.	150
2	Workshop on Advisory Mission on Search, Seizure, and Confiscation of Online Crime Proceeds at the Kempinski Gold Coast Hotel in Accra, from May 30 to June 01, 2022.	22
3	Global Internet Forum to Counter Terrorism (GIFCT) Workshop on Countering Terrorism and Violent Extremism Online in September 2022.	120
4	E-Evidence First Responder Trainer Course (EFR-TOT) spanning from June to July, 2022.	4
5	Introductory Training Course on Cybercrime for Judges and Prosecutors and training of trainers Part I, from December 6 to 9, 2022.	28
6	Launch of the 2022 edition of the Africa Safer Internet Day (ASID).	4,000
7	Seminar on how Civil Society Organisations (CSOs) may help with the effective implementation of the Cybersecurity Act, 2020 (Act 1038) organised by the Media Foundation for West Africa (MFWA).	100
8	Girls in ICT mentorship programme organised by the Ministry of Communications and Digitalisation.	1,000
9	Awareness Creation and Capacity Building Training for Teacher Mentors of Campaign for Female Education (CAMFED)on March 11, 2022.	31
10	Cybersecurity sensitisation exercises for religious groups in the country.	81,015
11	National Cyber Security Awareness Month (NCSAM) 2022.	15,557
	Total	102,027

The CSA over the year was committed to reaching the Ghanaian public, businesses and children with awareness creation materials in the form of Public Alerts, Advisories and discussion of various cybersecurity issues using the Mass media and Social media. These reached varied audiences across the country.

A DAILY GRAPHIC EDITORIAL OF SEPTEMBER 20, 2022

Daily Graphic, Tuesday, September 20, 2022.

SHOWBIZ Graphic SPORTS Mirror now Online!
Visit: www.graphic.com.gh/showbiz
www.graphic.com.gh/graphicsports
www.graphic.com.gh/mirror

Editorial 07

Daily Graphic
EDITORIAL

Tuesday, September 20, 2022

Digitally safe country necessary

LAST Thursday, the *Daily Graphic* reported the launch of the Cyber Security Month, which is scheduled to start from October 1.

The month-long awareness programme will have the Cyber Security Authority (CSA) touring the length and breadth of the country, sensitising Ghanaians to security online and digitally enabled technologies.

The theme selected for the awareness programme is: "Regulating cyber security: A public-private sector collaborative approach."

The month-long programme is part of the government's efforts under its five-year National Cyber Security Awareness Programme, dubbed: "A safer digital Ghana."

Essentially, cyber security is the protection of Internet-connected systems, such as hardware, software and data, from cyber threats.

The practice is used by individuals and enterprises to protect against unauthorised access to data centres and other computerised systems.

Indeed, a safer digital Ghana is all that Ghanaians crave for.

We look forward to a safer digital Ghana where digitally enabled technologies, such as the Internet and e-services are propelling dynamic economic growth and prosperity for all; where such technologies are used to extend healthcare services to remote locations; where students study unhindered by having access to data to also contribute towards better digitalisation nationwide.

We want a safer digital Ghana where all know the place of digitalisation as an enabler of societies and not a tool for profanity, insulting the elderly or engaging in crime or fraudulent activities.

The *Daily Graphic* had, in the past, used its voice to call for the sensitisation of Ghanaians to the security of the virtual world and we are happy that the government has such a plan.

Also very encouraging is the fact that the CSA will be carrying out activities with partners nationwide for a whole month.

Ensuring safety online or in the use of digitally enabled technologies is a collective effort of both the public and the private sectors.

That is because these sectors are linked and not independent of each other. Rather, they propel each other and any weakness in one sector impacts on the other.

Apart from that, cyber security issues, by necessity, need the collaboration of parties in both sectors because the virtual space is extensive and many a time faceless.

The theme for the month-long awareness is thus apt.

The *Daily Graphic* expects that at the end of October, the outcome of the month-long programme will include an army of common "cyber security aware Ghanaians" who are not only knowledgeable about cyber security but are also trainers of others, carrying onwards the message of cyber security.

We also expect that the month-long effort will be replicated next year and launched in our markets, commercial vehicle terminals (trotro stations), taxi ranks, churches and mosques.

The *Daily Graphic*, for its part, being the state's truthful and accurate mouthpiece, lends its support to the programme, ready to inform many more others as the programme rolls on.

This is because cyber insecurity is costly to the country, individuals and other economic actors.

Ayekoo CSA. Kudos for the efforts.


NATIONAL
CYBERSECURITY
CHALLENGE
who will be the
Cyber Hero?


NATIONAL
CYBER SECUR
AWARENE ONTH

Maiden Edition of the National Cybersecurity Challenge

The maiden edition of the National Cybersecurity Challenge (NCC) which was organised as part of the 2022 edition of the National Cyber Security Awareness Creation Month (NCSAM) to create awareness on child online safety practices through a quiz competition on cybersecurity-related issues among six (6) identified schools. The event was run as a pilot in preparation for a nationwide implementation in 2023.

Review of National COP Framework

The National COP Framework was reviewed and finalised in conjunction with relevant stakeholders to align with international best practices, the Cybersecurity Act, 2020 and to provide a holistic approach to address the challenge children face online. The framework provides the necessary guidelines and tools to all stakeholders involved in protecting children's rights online to ensure the full participation, protection and promotion of digital rights of Children in Ghana.

International Commitments to Child Online Protection

Ghana has received international recognition and has participated in a number of international conferences and meetings with international organisations due to its performance in the area of child online protection. Following the ratification of some international conventions like the African Union Convention on Cyber Security and Personal Data Protection and the membership of Ghana on the African Committee of Experts on the Rights and Welfare of the Child (ACERWC), the CSA over the year has been committed to providing a practical orientation of child rights online and ways to combat Child Sexual Exploitation and Abuse online.

Ghana is a member of the WePROTECT Global Alliance and has received some support that provides objectives and a comprehensive strategy for collaboration, coordination, and shared learning to eliminate Online Child Sexual Exploitation and Abuse (OCSEA) in the country. Through this alliance, Ghana has also contributed to knowledge on a number of international forums with regards to child online safety.

Stakeholders Engagements

The COP initiative in Ghana has achieved this great milestone based on strong collaboration and support of local stakeholders. The major stakeholders include the Ministry of Communications and Digitalisation, Ministry of Gender, Children and Social Protection, Ministry of Education, Judicial Service, Office of the Attorney General's Department and Ministry of Justice, Ghana Police Service, and Civil Society Organisations such as Child Online Africa. In 2022, the Authority met with stakeholders on various platforms including the Development Partners Forum and a Seminar with Civil Society Organisations.

Digital Literacy Package

In partnership with the Guidance and Counselling Unit of the Ghana Education Service, the Cyber Security Authority has contributed to the development of the digital literacy package aimed at educating school children about the responsible utilisation of digital tools.

Operationalisation of the Internet Watch Foundation (IWF) Reporting Portal

The Cyber Security Authority with support from UNICEF Ghana has operationalised the Internet Watch Foundation (IWF) Reporting Portal which enables reporting and takedown procedures of images and videos of illegal content children and young people encounter online.

Awareness Creation for Children

The Authority has been cautious about awareness creation programmes targeting children. A number of such sessions have therefore taken place in Junior and Senior High Schools as well as in schools that have children with special needs like the Akropong School of the Blind.

A lot of such awareness creation programmes have also been through the Mass and Social Media targeting parents, teachers and children eg. The 2022 Africa Safer Internet Day celebration was mainly media driven and covered audiences across the country using English and other local languages.

The table below shows the number of children and young people reached through these campaigns

Year	Total
2018	7,384
2019	39,334
2020	750
2021	NA (COVID-19)
2022	4,982
Sub Total	52,450

International Cooperation Milestones

Pursuant to Section 83 of the Cybersecurity Act, 2020 (Act 1038), the Authority carried out a number of international cooperation activities in 2022. These include:

United Nations Activities

The Cyber Security Authority has been participating in the United Nations Open Ended Working Group since 2015. In 2022, efforts were made to make active contributions and continue to share best practices in capacity building, confidence building measures, international cooperation among others with member states. Additionally, the Authority facilitated Ghana's representation at an informal breakfast session to explore how the work of the Freedom Online Coalition (FOC) can contribute to that of the Open-ended Working Group on security of and in the use of information and communications technologies (OEWG 2021-2025) in New York.

The Authority further participated actively in the United Nations Ad hoc committee on elaborating a comprehensive international convention on countering the use of ICTs for criminal purposes. The team also joined in the Open-Ended Working Group on the security of and in the use of ICTs. In these meetings, Ghana contributed to ensuring that the future convention contains adequate substantive law, procedural and international cooperation measures aimed at harmonising cybercrime laws among member states and promoting mutual legal assistance for the successful prosecution of cybercrimes. The Ghanaian delegation is particularly working hard to ensure that the convention contains provisions that criminalises illicit conduct against Critical Information Infrastructure, criminalisation of child exploitation and abuse as well as online offences that disproportionately affect women and girls.

The CSA over the year effectively worked with the Ghana High Commission in Vienna and New York through the Ministry of Foreign Affairs and Regional Integration to enable a smooth participatory process in all the sessions and to ensure that Ghana's contributions are in line with country's foreign policy.

Council of Europe Activities

The Authority in 2022 engaged with relevant partners to facilitate the process of signing the Second Additional Protocol to the Budapest Convention. Additionally, under the Global Action on Cybercrime Extended (GLACY+), CSA facilitated Ghana's representation at the Interpol Digital Security Challenge in Singapore and at Interpol's 9th Africa Working Group Meeting on Cybercrime for Heads of Units and Workshop on channels and avenues for international cooperation in cybercrime. The Authority further hosted the GLACY+ Workshop on Search, Seizure and Confiscation of Online Crime Proceeds in Accra.

Global Forum on Cyber Expertise

The CSA had several engagements with the Global Forum on Cyber Expertise (GFCE) and participated in various working groups within the Forum. The CSA additional facilitated the hosting of the African Union (AU)-Global Forum on Cyber Expertise (GFCE) Kick-Off Meeting and an Executive Course on International Law of Cyber Operations funded by the Government of Canada in partnership with Cyber Law International, both in Accra.

Freedom Online Coalition

The CSA participated at RightsCon, the Digital Rights Inclusion Forum (DRIFF) 22 and other events as members of the Freedom Online Coalition. Ghana also continued its work as the sole Chair of the Task Force on Digital Equality (TFDE) and led conversations around digital equality. As Chair, efforts were made to organise a learning call with renowned scholar, Nani Jansen Reventlow.

Global Internet Forum to Counter Terrorism (GIFCT)

As a result of Ghana's membership in the GIFCT, CSA participated in GIFCT related meetings and partnered with the GIFCT and Tech against Terrorism (TaT) to organise a Multi-Sector Workshop on "Countering Terrorism and Violent Extremism Online" in Accra. The event brought together law enforcement agencies to increase its engagement with Ghana to better understand how the tech/extremism nexus manifests itself, not only in Ghana but also in West Africa and the rest of the African continent.

Bilateral Relations

In 2022 alone, Ghana through the CSA received delegations from 3 African countries (The Gambia, Sierra Leone and Mozambique) and they sought collaborations and support to develop key cybersecurity initiatives in their respective countries. Ghana also held bilateral meetings with Singapore and Saudi Arabia and hope to sign MOUs with them soon for further collaborations in cybersecurity development.

In 2022, the Authority signed a Memorandum of Understanding (MoU) with the National Institute of Information and Communication Technology (INTIC) of Mozambique and the National Cyber Security Authority (NCSA) of Rwanda to strengthen collaborative and capacity building efforts.

Locally, the CSA engaged in courtesy calls Denmark, European Union (EU) Commission, Canada, Italy and Czech Republic

Other Activities

For the year 2022, Ghana, represented by the Cyber Security Authority (CSA) chaired the Freedom Online Coalition (FOC) Task Force on Digital Equality (TFDE),

served on the FOC Friends of the Chair and served as a member of the FOC Task Force on Artificial Intelligence and Human Rights.

The CSA represented Ghana at the 10th edition of the African School on Internet Governance (AfriSIG2022) which took place from July 16-18, 2022 as the pre-event to the African Internet Government Forum held in Lilongwe, Malawi which was focused on international cybersecurity.

The CSA signed an MoU with the Elizabeth Sloan Institute for cybersecurity training and capacity building.

The CSA has also contributed to knowledge sharing across the globe through its speaking roles and presentations at international workshops and webinars organised by the World Bank, World Economic Forum, among others. For instance over the year, Ghana participated actively in the Cybersecurity Summit in Lome, World Economic Forum Annual Meeting, the Singapore Cybersecurity Week, Global Cybersecurity Forum in Saudi Arabia, among many more.

Finance & Administration Activities

The Authority through these functional areas implemented a number of key initiatives in relation to its mandate. These include the following:

- Identification and development of IGF sources. The Ministry of Finance has been engaged in the development of IGF pursuant to Section 23 of Act 1038.
- Establishment of the Entity Tender Committee pursuant to section 20(1) of the Public Procurement (Amended) Act, 2016 (Act 914). This is to ensure compliance with procurement activities and procedures prescribed in the Act.
- Established a Fixed Asset Coordinating Unit and compiled records on Fixed Asset pursuant to Section 154 to 156 of the Public Financial Management (PFM) Regulation, 2019 (L.I. 2378).
- Development and maintenance of books of accounts and records on the Sub-Consolidated and other funds.
- Implementation of GIFMIS for GoG transactions.
- Facilitated the execution of an Interim Financial Statements Audit from October 2021 to August 2022.
- Established and obtained approval (Warrant) for Standing Imprest system pursuant to Section 98 of the Public Financial Management (PFM) Regulation, 2019 (L.I. 2378).
- Development of policies such as the Organisational Manual, Conditions of Service, Schemes of Service, Leave Policy.
- Approved Establishment Levels from Public Services Commission for regularisation of staff.

Summary of Financial Results

An amount of GH₵2,263,037.15 (GH₵365,958.87 for the Use of Goods and Services and GH₵1,897,078.28 for Capital Expenditure) was released by the Ministry of Finance during the 2022 financial year out of a total revised allocated amount of GH₵11,515,000.00 (GH₵3,115,000.00 for the Use of Goods & Services and GH₵8,400,000.00 for Capital Expenditure) for cybersecurity related activities of the CSA. The overall budgeted Year-to-Date amount for the 2022 financial year is GH₵33,740,315.44 and the Year-to-Date expenditure amounted to GH₵10,404,565.00.

The Authority was mainly supported by the National Communications Authority (NCA), the World Bank through the e-Transform Ghana Project and Child-Online Protection (COP)-specific project support from UNICEF, National Cyber Security Awareness Month (NCSAM 2022) Partners/ Sponsors and Plan International for the 2022 financial year.

Management Letter/Audit Report

The Financial Accounts of the Cyber Security Authority for the period October 2021 to December 2022 have been audited in accordance with Article 187(2) of the 1992 Constitution and Section 11(1) of the Audit Service Act, 200 (Act 584), the Auditor has provided a Management letter and the Accounts are yet to be signed.

Challenges

- As a young agency under the Ministry of Communications and Digitalisation, The Authority has a number of challenges mainly financial due to insufficient budgetary allocation by the Government of Ghana to run its operations.
- Logistical constraints in the form of operational vehicles, laptops and other equipment slowed down work in the Authority.
- Limited Office Space for management and staff of the Authority.
- Challenges getting venues with required specifications to host international events; leading to change of dates and in most cases, other countries were nominated to host the intended events.

THE FUTURE OUTLOOK OF THE AUTHORITY

National CERT

- Enhancement of collaboration with identified priority countries including Rwanda, Mozambique, Singapore, Mauritius and Tanzania to share knowledge on best practices on incident response measures among other key CERT related mandate.
- Operationalisation of Ghana's membership of AfricaCERT and the Forum of Incident Response and Security Teams (FIRST).
- Deployment of an Information Sharing Platform for various Sectoral CERTs.
- Collaboration with other accredited CERTs for the development of sector specific regulatory directives for Sectoral CERTs.
- Implementation of the Accreditation Framework for Sectoral CERTs.

Critical Information Infrastructure (CII)

- Registration of all Designated CII and the implementation of Audit and Compliance programmes.
- Development and implementation of Risk and Crisis Management Frameworks for designated CIIs and Government Digitalisation Initiatives.
- Development of Sectoral Directives for key CII sectors including the Government Sector, Energy Sector; Health Sector; the Financial Sector and the Telecommunications Sector.

Child Online Protection (COP)

- Launch and implementation of the National Child Online Protection Framework.
- Awareness creation and sensitisation programme on cyber hygiene practices and the COP-related provisions in the Cybersecurity Act, 2020 (Act 1038) for children, parents and other key stakeholders.
- Implementation of the National Cybersecurity Challenge programme in collaboration with key stakeholders and partners.
- Local cooperation and deployment of technology system to facilitate reporting and threat analysis of child online safety issues.
- Launch and implementation of the COP Guidelines for Children, Parents, and Educators.

Law Enforcement and Liaison

- Development & implementation of Data Retention Framework for Service Providers pursuant to Section 77 of Act 1038.
- Support with the development of specifications for Interception Capability for Service Providers pursuant to Section 76 of Act 1038.
- Development & Implementation of Data Retention Technology Framework for Service Providers pursuant to Section 77 of Act 1038 in collaboration with Cybersecurity Technology Standards.
- Development of Technology Specifications for Interception Capabilities for Service Providers in collaboration with other JCC members including the NCA, National Signals Bureau, CID, etc. pursuant to Section 76 of Act 1038 in collaboration with Cybersecurity Technology Standards.

Legal and Compliance

- Coordinate the Development of Legislative Instrument (L.I) for the Cybersecurity Act, 2020 (Act 1038).
- Implement the Framework for the Licensing of Cybersecurity Service Providers, Accreditation of Cybersecurity Establishment, and Accreditation of Cybersecurity Professionals.
- Development and Adoption of Data Protection & Right to Information Policy/Protocols pursuant to the provisions of the Data Protection Act, 2012 (Act 843) and the Right to Information Act, 2019 (Act 989), among other activities.

Cybersecurity Technology Standards

- Development of baseline cybersecurity specifications and cybersecurity guidance on specific technology by government, children, the public, businesses, etc.
- Development & Implementation of Data Retention Technology Framework for Service Providers pursuant to Section 77 of Act 1038
- Implementation of the Rayzone's project.

Others

- CSA looks forward to the adoption and implementation of the National Cybersecurity Policy and Strategy (NCPS).

Administration

- Implement Administration related policies & procedures including:
  - Scheme of Service
  - Condition of Service for Staff
  - HR Manual/Policy
  - Job Description (JD) for Staff
- Implement staff performance management system for the CSA
- Develop and implement Code of Conduct for the CSA
- Develop and implement Procurement Plan and Policy for the CSA
- Compilation of Asset Register and regular inventory updates
- Procurement of logistical items for the operations of the CSA
- Operationalise international cooperation treaties/agreements including MoU with the State of Israel, Singapore, Mauritius, GFCE, and World Economic Forum.

Finance

- Development & adoption of financial administration related policies & procedures.
  - Financial Administration Manual/Policy
  - Internal Control Policy
  - Development Partners Financial Support Policy
- Automation of payment of compensation/salaries of Staff on Government Payroll.
- Coordinate the establishment of the Cybersecurity Fund
- Implementation of Internally Generated Funds (IGF) in accordance with Section 23 of the Cybersecurity Act, 2020 (Act 1038).

Internal Audit

- Establishment of an Audit Committee for the CSA pursuant to Section 86(1) of the PFM Act, 2016 (Act 921).
- Development of Risk Management Policy, Risk Register & Guidelines for the CSA in accordance with Section 83(4) of the PFM Act, 2016 (Act 921).

CORPORATE INFORMATION

Board Chairperson	Hon. Ursula Owusu-Ekuful, Ministry for communications and Digitalisation
Director-General	Dr. Albert Antwi-Boasiako
Board Secretary	Ms. Efua Brown-Eyeson
Office	3rd Floor, NCA Towers, KIA, 6 Airport Bypass Road, Accra. GL-126-7029
Email Address	info@csa.gov.gh
Telephone	(+233) 303972530 / (+233) 303972531

CYBER SECURITY AUTHORITY
FREEDOM AND JUSTICE
CSA

CYBER SECURITY AUTHORITY

www.csa.gov.gh

A SAFER DIGITAL GHANA