'23

ANNUAL REPORT

CYBER SECURITY AUTHORITY (CSA)

www.csa.gov.gh

A SAFER DIGITAL GHANA

CYBER SECURITY AUTHORITY
FREEDOM AND JUSTICE
CSA

TABLE OF CONTENT

TABLE OF CONTENT

Acronyms

ANCA	Africa Network of Cybersecurity Authorities
APR	Annual Progress Report
ASID	Africa Safer Internet Day
CBAC	Capacity Building and Awareness Creation
CEs	Cybersecurity Establishments
CERT	Computer Emergency Response Team
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CPs	Cybersecurity Professionals
CSA	Cyber Security Authority
CSPs	Cybersecurity Service Providers
DPC	Data Protection Commission
ETC	Entity Tender Committee
FICSOC	Financial Industry Command Security Operations Centre
FIRST	Forum of Incident Response and Security Teams
FOC	Freedom Online Coalition
FOC	Freedom Online Coalition
GARNET	Ghanaian Academic Research Network
GC3B	Global Conference on Cyber Capacity Building
GDAP	Ghana Digital Acceleration Project
GDIs	Government Digitisation Initiatives
GFCE	Global Forum on Cyber Expertise
GLACY+	Global Action on Cybercrime Extended
GLACY-E	Global Action on Cybercrime Enhanced
IGF	Internally Generated Funds

IRMS	Implementation of Integrated Regulatory Management
JCC	Joint Cybersecurity Committee
LECO	Legal and Compliance
LELU	Law Enforcement Liaison Unit
LI	Legislative Instrument
MOCD	Ministry of Communication and Digitalisation
NCA	National Communications Authority
NCC	National Cybersecurity Challenge
NCSAM	National Cyber Security Awareness Month
NCSC	National Cyber Security Centre
NCSS	National Cyber Security Secretariat
NITA	National Information Technology Agency
NSB	National Signals Bureau
OCSEA	Online Child Sexual Exploitation and Abuse
PFM	Public Financial Management
PPA	Public Procurement Authority
RTP	Restrictive Tendering Procedure
SOP	Standard Operating Procedures
TAIEX	Technical Assistance and Information Exchange
TFDE	Task Force on Digital Equality
TOR	Term of Reference
UNICEF	United Nations International Children's Emergency Fund
UN-OEWG	United Nations Open-Ended Working Group

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 (CII) in respect of cybersecurity activities, cybersecurity service providers and practitioners in the country;
- Promote the development of cybersecurity in the country to ensure a secure and resilient digital ecosystem;
- Establish a platform for cross-sector engagement on matters of cybersecurity for effective co-ordination and cooperation 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

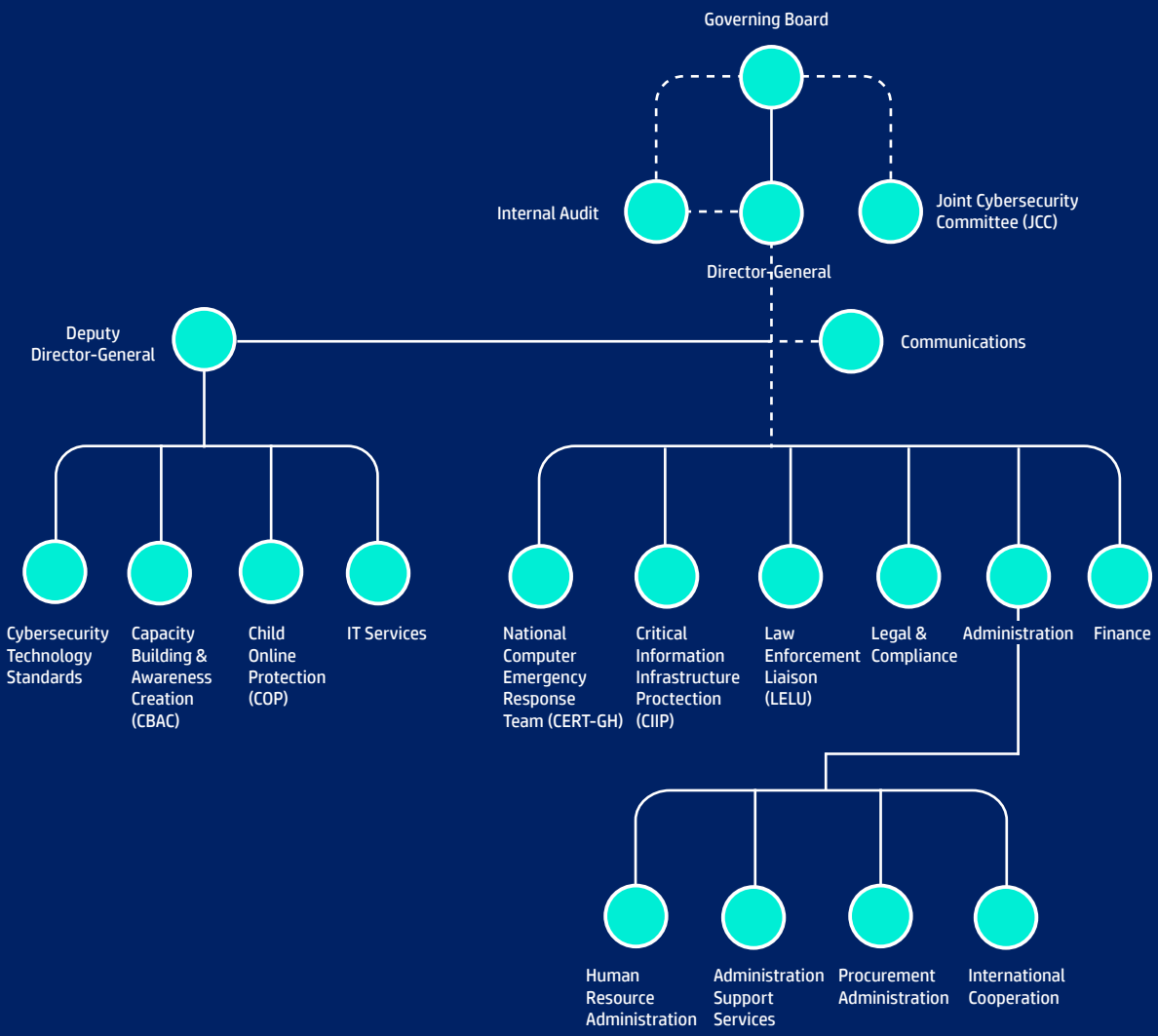
FUNCTIONS OF THE AUTHORITY

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 the 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

PROFILES 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.

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.

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.

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 MANAGEMENT TEAM

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

REPORT

By Chairperson of the Governing Board

Introduction

It is with great pleasure that I present the Annual Report of the Cyber Security Authority (CSA) for the year 2023 as the Board Chair of the Authority, in accordance with section 28 of the Cybersecurity Act, 2020 (Act 1038).

The Cyber Security Authority was established by the Cybersecurity Act, 2020 (Act 1038) to regulate cybersecurity activities in Ghana, and two years after its inception, it has advanced Ghana's digital landscape and ensured cybersecurity resilience in our nation through its regulatory activities.

Cybersecurity Regulations

In 2023, the CSA begun implementing various initiatives to protect the digital ecosystem as mandated by law. These include the implementation of the regulatory regime of licensing Cybersecurity Service Providers (CSPs), the accreditation of Cybersecurity Establishments (CEs) and the accreditation of Cybersecurity Professionals (CPs).

To ensure the protection of Critical Information Infrastructures (CIIs), given the current digital transformation agenda, there is an ongoing registration of designated CII owners and the response of stakeholders has so far been impressive.

To ensure oversight supervision of the operations of the Sectoral CERTs and compliance with incident reporting obligations across diverse sectors, the guideline for the accreditation of Sectoral CERTs has been developed and submitted for consideration by the Governing Board. We will give it the necessary attention for subsequent implementation.

We are grateful to the state for the financial clearance given the Authority to regularise its staff and to employ additional staff to support the work of the Authority. This is a very significant milestone for a young institution like the CSA.

International Cooperation

In 2023, Ghana hosted the maiden Global Conference on Cyber Capacity Building (GC3B) in November which led to the signing of the Accra Call. The Call aims to stimulate global action to elevate cyber resilience across international and national development agendas and promote cyber capacity building that supports broader development goals. Hosting the Global Conference on Cyber Capacity Build (GC3B) in Accra was quite significant as it signified Ghana's global recognition for its leadership in cybersecurity development.

Also worth noting during the year under review is the election of Ghana to chair the Africa Network of Cybersecurity Authorities (ANCA). Ghana is committed to leveraging this platform to inspire the continent to initiate bold measures within the cybersecurity space.

Outlook for 2024

In the forthcoming year, the Authority will maintain its commitment to implementing all regulatory interventions as mandated by the Cybersecurity Act, 2020 (Act 1038).

We eagerly anticipate the finalisation and approval of two Legislative Instruments (LIs) which have been initiated to complement the operationalisation of Act 1038 and staff conditions of service.

The Board has a keen interest in the establishment of the Industry Forum to create a platform that will bring industry together to discuss matters of common interest to the industry. We are committed to providing the needed oversight to ensure its realisation in accordance with Section 81 of the Cybersecurity Act, 2020 (Act 1038).

Acknowledgements

The Authority's performance in 2023 has been commendable, and I extend my heartfelt appreciation to the Board, Management, and staff for their unwavering diligence and dedication in the past year.

Furthermore, I am deeply grateful to His Excellency, President Nana Addo Dankwa Akufo-Addo, and Vice President Alhaji Dr. Mahamudu Bawumia for their steadfast commitment to digital advancement and safeguarding our digital assets.

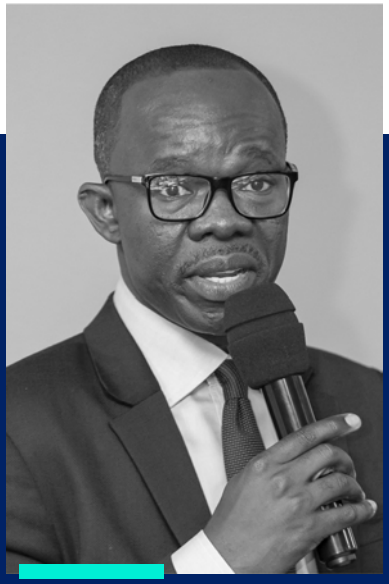
The members of the CSA Governing Board have been instrumental in driving the CSA's growth despite the limited resources and I am grateful for the support.

Lastly, I express gratitude to all private and public sector stakeholders for the continuous support and collaboration, which are essential in building a resilient and secure digital Ghana.

Hon. Mrs. Ursula Owusu-Ekuful
Chairperson, CSA Governing Board
December, 2023

REPORT

By Director-General



Background

As we reflect on 2023, I am elated to share that our unwavering commitment to safeguarding our digital infrastructure and cyberspace as a young institution has yielded remarkable strides. Through the strategic allocation of limited resources and fostering partnerships with both public and private stakeholders, we have sustained our operations and advanced in executing our mandate as the regulator of cybersecurity activities in the country as stipulated in the Cybersecurity Act, 2020 (Act 1038).

Licensing and Accreditation of CSPs, CEs and CPs

The process of licensing Cybersecurity Service Providers (CSPs), and accrediting Cybersecurity Establishments (CEs) and Cybersecurity Professionals (CPs) commenced in March 2023 pursuant to sections 49-59 of the Cybersecurity Act, 2020 (Act 1038). Following the extension of an initial deadline of September 30, 2023, to December 31, 2023 for all CSPs, CEs and CPs to comply with the provisions of the Act, I am happy to say the project has been largely successful, exceeding the Authority's set target. As of December 2023, 1,261 businesses and individuals operating in the country had registered with the CSA to seek licenses and accreditation in compliance with the regulatory regime.

Critical Information Infrastructure Registration

In 2022, the Authority commenced registration procedures for institutions designated as critical information infrastructure pursuant to sections 35-40 of (Act 1038). In 2023 significant progress was made in this direction with the majority of CII owners complying with the requirements of the Act and the Directive for the protection of CIIs.

Incident Reporting Points of Contact (PoC)

The Cybercrime/Cybersecurity Incident Reporting Points of Contact have been operating since October 2019. Since its establishment, the PoCs have proved to be a means of preventing crimes or ensuring that the populace does not fall prey to online crimes. It thus offers guidance and advice to prevent and assist in dealing with cybercrime incidents. In 2023, a total of 13,353 contacts were made to the CSA through the PoCs. Out of this number, 1,255 were actual cyber-related incidents while 12,098 were requests for direct advisories.

International Cooperation

The CSA, recognising the importance of cross-border collaboration in the fight against cybercrimes, actively engaged in international cooperation activities in 2023. Amongst the international cooperation milestones over the period were Ghana's leadership within the Freedom Online Coalition (FOC) as chair of the Task Force on Digital Equality (TFDE), and the signing of the Second Additional Protocol to the Budapest Convention on Cybercrime. The Authority also participated in key United Nations committees such as the Adhoc Committee and United Nations Open-Ended Working Group (UN-OEWG) on the Security of and in the Use of ICTs. Worth noting is Ghana's hosting of the inaugural edition of the Global Conference on Cyber Capacity Building (GC3B). The two-day event brought about 800 participants to Ghana and led to the signing of an outcome document, the "Accra Call for Cyber Resilient Development".

Furthermore, the outcome document on Ghana and the World Bank's collaboration in cybersecurity, which explores how Ghana has become a regional leader in cybersecurity, was launched at the GC3B Conference. The document focuses on the key milestones and decisions made by Ghana's government, the results delivered to Ghana's economy and society, and the lessons learned that could be applied by other countries seeking to strengthen their cyber resilience.

Ghana was also selected to chair the Africa Network of Cybersecurity Authorities (ANCA): a dedicated platform for African countries with established National Cybersecurity Authorities to collaborate on cybersecurity matters.

Child Online Protection

Ensuring the protection of children online continues to be of paramount importance to the CSA. The National Child Online Protection Framework has been finalised by stakeholders and sent to cabinet for approval. The 2nd edition of the National Cybersecurity Challenge (NCC) drew participants from 50 Senior High Schools across Ghana, a massive build-up on the initial 6 schools that participated in the maiden edition, to promote awareness amongst children and ensure the active participation of children in cybersecurity-related matters.

Capacity Building and Awareness Creation

The CSA, in accordance with section 60 of the Cybersecurity Act, 2020 (Act 1038), delivered on its mandate to enhance public awareness and education on cybersecurity matters. Throughout 2023, the CSA conducted several sensitisation workshops for private and public institutions to build their capacity on cybersecurity matters. There was also the successful execution of the 2023 National Cyber Security Awareness Month (NCSAM), organised under the theme, "Promoting a Culture of Digital Safety". This month-long initiative focused on fostering a culture of cybersecurity among Ghanaians, addressing the consequences of unsafe digital practices, enhancing collaboration among stakeholders, and equipping the populace with the necessary skills to combat cybercrimes. These initiatives emphasised the CSA's commitment to strengthening cybersecurity resilience across the nation, recognising that a society's cybersecurity is only as robust as its weakest link.

Human Resource

In 2023, the Governing Board of the CSA chaired by Hon. Mrs. Ursula Owusu-Ekuful, who doubles as the Minister for Communications and Digitalisation was very instrumental in facilitating the regularisation and the approval to employ 100 staff.

The Way Forward

Ghana remains at the forefront of cybersecurity initiatives in Africa, inspiring sister nations. As we embark on the journey into the future, we recognise that the cybersecurity landscape will continue to evolve, presenting new challenges and opportunities. Despite the dynamic nature of the cyber landscape, we remain steadfast in our commitment to safeguarding Ghana's digital assets and promoting a secure cyber environment for all citizens.

In 2024, the Authority is set to implement pivotal policies and initiatives to safeguard the digital ecosystem. Among these measures is the implementation of a comprehensive Framework for the Accreditation of Sectoral Computer Emergency Response Teams (CERTs), enhancing our ability to promptly manage cyber threats and coordinate incident responses across different sectors of the economy. Concurrently, the rigorous enforcement of Guidelines for the Licensing of Cybersecurity Service Providers, Accreditation of Cybersecurity Establishments, and Accreditation of Cybersecurity Professionals will continue in earnest.

Additionally, efforts to protect our most vulnerable demographic: children, will intensify with the implementation of the National COP framework. The Authority will also amplify its awareness creation campaigns to ensure that more citizens are cyber-conscious.

Our primary aim is to propel Ghana to greater heights on the global cybersecurity stage. The dedicated team at the Cybersecurity Authority (CSA) is unwavering in its pursuit of Vision 1:25 – a vision that aims to establish Ghana's cybersecurity infrastructure as the foremost in Africa and among the top 25 globally.

Acknowledgement

I extend my sincere gratitude to all our stakeholders, the Governing Board and the dedicated staff whose unwavering support and commitment have been instrumental in our growth as an institution. I eagerly anticipate collaborating with all relevant stakeholders to shape a safer and more secure digital future for all.

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's Governing body was inaugurated in February 2022.

Pursuant to section 5(1) of (Act 1038), the governing body of the Authority is a Board consisting 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 and 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

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 2023.

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 and 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 Protection (CIIP) 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 Audit and Compliance Monitoring of CII in adherence to the CII Directive, and acting as a point of contact between CIIs Owners and the CSA on all CII engagements.

Capacity Building & Awareness Creation (CBAC)

Pursuant to section 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 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 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 through collaboration with stakeholders; implementing the COP project - a collaboration between the Ministry of Communications and Digitalisation, Ministry of Education, Ministry of Gender, Children and Social Protection, and the UNICEF Ghana. Other roles include;

- Implementing the 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, Accreditation, and Certification of Cybersecurity Service Providers and 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 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. In addition to the above, the Administration functional area provides Administrative Support Services including transport, estate, and security for the Authority. The functional area also plays an oversight role for Human Resource Administration and Procurement related matters. Similarly, the Administration the functional area plays an oversight role for International Cooperation Unit of the CSA to secure cyberspace through international collaborations in line with section 83 of the Cybersecurity (Act 1038).

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 functional area 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.

Report

ADMINISTRATION

Human Resources

Workforce Planning, Staff Turnover and Retention

During the reporting year, the Authority commenced the regularisation of staff after securing the financial clearance from the Ministry of Finance. As of December 2023, ninety (90) staff had been regularised as staff of the Cyber Security Authority.

Over the year 2023, a total number of eight (8) staff (4 males and 4 females) exited from the Authority. The reasons for the separation were mainly due to pursuing further studies. In addition, two (2) seconded officers ended their term of service with the Authority.

The workforce composition as at December 31, 2023, is as follows:

Category	Male	Female	Total
Regularised	56	44	90
Secondment	8	6	14
Contract/ Consultants	3	2	5
National Service	2	1	3
Total	69	53	122
(%)	57%	43%	100%

Staff Training and Development

The CSA believes that training and development is fundamental to staff performance, through collaborative efforts staff were given various competency-based and skills development training.

The Authority also granted study leave for staff who have been awarded scholarships to undertake various master's degree programmes required by the schemes of service. Some categories of staff were also supported to pursue higher education through flexible work arrangements.

Staff Compensation

Having regularised ninety (90) staff on to the Government of Ghana payroll system, all the ninety staff were paid through the Integrated Personnel Payroll Database (IPPD). Seconded officers continued to receive their salaries from their primary organisations, with the Authority disbursing approved allowances to them. Contract staff were paid through government subventions whilst consultants were paid through the e-Transform (World Bank) Project.

24-Hour Shift System

Pursuant to Section 48(1) the Authority is mandated to establish a cybersecurity incidents point of contact to facilitate reporting of cybersecurity incidents by the general public. By implication, the National Computer Emergency Response Team (CERT-GH) will require manpower to be able to achieve this mandate. For this reason, the CSA beefed up the needed manpower to enable the CERT-GH to provide 24-hour service to the general public.

Procurement and Purchasing

Procurement transaction for 2023/2024

Procurement by Method

Method	No. of Contract Issued	Percentage Per Value
Restrictive Tendering Procedure (RTP)	22	41.51%
Single/Sole Sourcing	1	1.89%
Shopping/RFQ	30	56.60%
Total	53	100%

Procurement by Method

Category	No. of Contract Issued	Percentage Per Value
Goods	9	18.37%
Services	40	81.63%
Total	49	100%

Establishment of the Entity Tender Committee (ETC) Meetings as per the Public Procurement Act 663

The Authority organised four quarterly Entity Tender Committee (ETC) meetings as required 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.

The Procurement functional area coordinated the development of the Workplan and Terms of Refence (TORs) for the Ghana Digital Acceleration Project (GDAP), a new world bank project under the auspices of MOCD on behalf of the CSA.

OVERVIEW OF 2023 OPERATIONAL PERFORMANCE

Implementation of Guidelines 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 Guidelines 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 CSA commenced the implementation of the Guidelines in March 2023.

Registration of Critical Information Infrastructure (CII)

Following the publication of Gazette Notice No. 132 in September 2021, institutions across 13 sectors have been identified and designated by the Minister as Critical Information Infrastructure (CII) owners and sectors, respectively. The CSA has conducted an analysis to identify potential institutions which qualify as CII Owners for the attention of the sector minister for possible designation pursuant to section 35 of Act 1038. The registration of all CIIs is implemented after the designation of the institutions.

The CII Registration process being undertaken is pursuant to section 36 of Act 1038 and Gazette Notice No. 140. The CII registration process involves the following major milestones:

- Nomination of CII Point of Contact
- Capacity building workshops on the CII Registration Process
- Completion and submission of CII Registration Form
- Validation of CII Registration Form
- Issuance of the Certificate of Registration

Milestones for CII Registration	Current Update
Nomination of CII Point of Contact	93% of CII Owners have nominated their CII Point 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
Completion and submission of CII Registration Form	53% of CII Owners have submitted the details of their critical systems to the CSA.
Validation of CII Registration Form	37% of CII Owners have held meetings with the CSA to validate the details of the submitted critical systems submitted.
Issuance of Certificate for Registration	This process is ongoing

Risk Assessment Framework for Critical Information Infrastructure (CII)

As part of efforts to operationalise section 59 of Act 1038, the Authority developed the first draft of the Risk Assessment Framework for Critical Information Infrastructure (CII), which outlined processes and procedures for conducting risk assessments to systematically identify and evaluate risks in CII environments.

To ensure collaboration and cooperation with CII Sectors and adoption of the Risk Assessment Framework, the Authority organised workshops with industry experts in 11 CII Sectors (Banking & Finance, Education, Emergency, Energy, Food & Agriculture, Government, Health, ICT, Manufacturing, Mining, and Transport). The workshops aimed to solicit input from the experts on the pertinent risks and the current processes used in managing risks in the respective sectors. The workshops span from May to July 2023, with 80% participation from the industry experts and CII Owners.

Implementation of Cybersecurity Technical Operations Infrastructure including Information Sharing Platform for Computer Emergency Response Team (CERT)

The CSA completed the racking and power-up of the hardware infrastructure at the NITA Data Centre. Network connectivity (leased line) was also established between the CSA office and NITA Data Centre to provide access to the infrastructure.

Implementation of Guidelines 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 draft Guidelines 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 Guidelines for the Accreditation of Sectoral CERTs is expected to be considered by the Governing Board for implementation, starting January 2024.

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

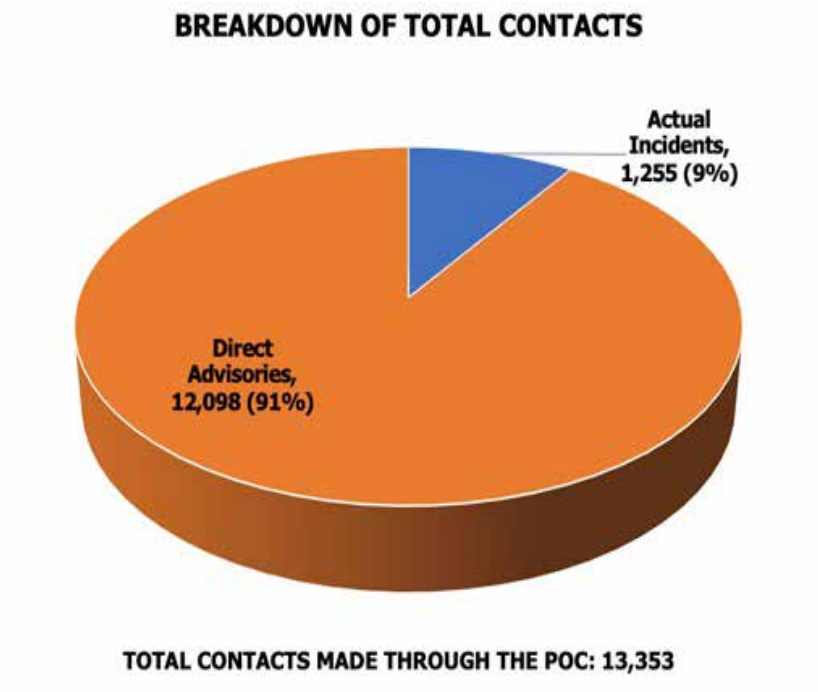
The Cybercrime/Cybersecurity Incident Reporting Points of Contact (PoC) was deployed in October 2019 to provide an avenue through which cybercrime/cybersecurity incidents and cases can be reported to the National Computer Emergency Response Team (CERT-GH) for analysis, investigation, and mitigation. The PoC serves constituents via six (6) channels: an Online Form, SMS, Call, E-mail, WhatsApp, and a Mobile Application.

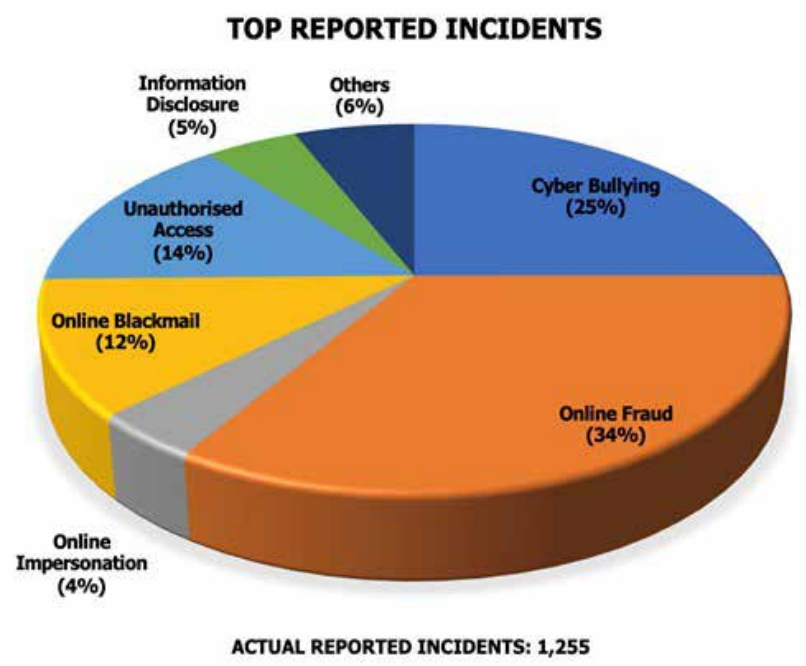
From January to December 2023, a total of thirteen thousand, three hundred and fifty-three (13,353) contacts were made with the CSA through the PoC. One thousand, two hundred and fifty-five (1,255) (representing 9%) constituted actual cyber-related incidents while 12,098 (representing 91%) were direct advisories. The top incident categories recorded over the period were:

- Online Fraud (34%) - schemes designed to take money off victims e.g. investment scams, online shopping fraud, job recruitment fraud, etc.
- Cyberbullying (25%) - the use of digital communication channels such as social media, and email to harass, threaten, embarrass, or target individuals or groups with the intent to harm them emotionally. The majority of the instances reported were associated with unauthorised loan apps.
- Unauthorised Access (14%) - gaining access to a computer system or services without the owner's permission typically through social engineering techniques e.g. account takeover (WhatsApp, Facebook, LinkedIn, etc.).
- Online Blackmail (12%) – the use of digital communication channels to threaten someone with the disclosure of sensitive, embarrassing, or private information or media unless a demand is met e.g. sextortion.

- Information Disclosure (5%) – information on cyber incidents shared by persons close to the actual victims or people who may have observed the incident and are thus providing a tip-off e.g. scam messages shared on social media.
- Online Impersonation (4%) - fraudulently using identities of high-profile personalities such as Ministers, Members of Parliament, and other politicians.

Below is a graphical representation of the PoC statistics.





- From a gender standpoint, seven hundred and sixty-eight (768) of the incidents (representing 61%), impacted males while four hundred and eighty-seven incidents (487) (representing 39%) impacted females.
- Seven (7) cases of Online Child Sexual Exploitation and Abuse (OCSEA) were reported during the year under review.

The Authority issued advisories to help protect individuals. The advisories issued through the PoC covered Children, the Public, Businesses, and Government institutions. Examples include:

- How to protect online accounts (bank accounts, emails, social media) from being compromised by enabling two-factor authentication, creating strong passwords etc.
- How to detect common online fraudulent schemes among others.

These advisories have been instrumental in helping constituents avoid becoming victims of cybercrime.

The CSA commenced collation of the monetary losses incurred by victims of cybercrime/cyber incidents during 2023. At the end of the year, four hundred and forty-six (446) incidents resulted in a loss of fifty-nine million, nine hundred and twenty-four thousand, eight hundred and thirty-seven Ghana Cedis (GHS 59,924,837). The distribution of the losses by incident category is shown in the following table:

S/N	Incident Category	Incident Count	Audience
1	Online Fraud	397	59,694,192
2	Online Blackmail	43	111,378
3	Online Impersonation	3	45,319
4	Unauthorised Access	3	11,300

Maiden National Cyber Drill

The CSA organised the maiden edition of a national cyber drill involving the National CERT and Sectoral CERTs as part of the 2023 edition of the National Cyber Security Awareness Month (NCSAM). The participating institutions included 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).
The objectives for the tabletop exercise were to:

- Examine the preparedness of Sectoral CERTs to protect themselves and their constituents from a DDoS attack.
- Examine the information sharing protocols of Sectoral CERTs with internal and external stakeholders and partners, particularly the National CERT.
- Assess the plans of Sectoral CERTs to detect, respond to and recover from a DDoS attack.
- Review the reporting protocols of Sectoral CERTs considering the provisions of Cybersecurity Act, 2020 (Act 1038).
- Assess the communications plans of Sectoral CERTs to respond to inquiries from the public and media regarding a DDoS attack.

Capacity Building and Awareness Creation

National Cyber Security Awareness Month (NCSAM) 2023

The National Cyber Security Awareness Month (NCSAM) is a flagship initiative under thefive-year National Cybersecurity Awareness Programme dubbed, "A Safer Digital Ghana". The programme focuses on four main pillars, thus Children, the Public, Businesses and Government. The 2023 edition of NCSAM was organised under the theme “Promoting a Culture of Digital Safety”. The event aimed at boosting public awareness and promoting responsible digital practices for a safer, more inclusive digital environment marked by respect, privacy protection, and ethical conduct. The month-long event focused on key areas of Ghana’s cybersecurity development discussed in forty-four (44) sessions.
The following are some of the activities and programmes organised during the month-long event:

- Media Launch of the National Cyber Security Awareness Month (NCSAM) 2023
- Official Launch of the National Cyber Security Awareness Month (NCSAM) 2023
- Workshop on Critical Information Infrastructure (CII) Security and Risk Management
- Public Consultation on the Accreditation of Sectoral Computer Emergency Response Teams (CERT)
- Cyber Drills on National Incident Response
- Impact of Disinformation on Electoral Integrity, Peace and Security
- Introductory Course on Cybercrime and Electronic Evidence for Judges and Prosecutors in Ghana.
- Legislative Instrument validation meeting
- Collaborative events with the Joint Cybersecurity Committee institutions.

Child Online Protection (COP)

On COP development, the Authority implemented several activities, including the following:

- The 2023 edition of the National Cybersecurity Challenge (NCC) to create awareness of child online safety practices through a competition on cybersecurity-related issues among fifty (50) senior high schools. The event was categorised into regional and zonal competitions and climaxed with the national finals in Acccra.
- Finalisation of the National COP Framework by stakeholders for cabinet approval.
- Commemoration of the Africa Safer Internet Day (ASID) in February 2023.
- Awareness creation and capacity building on the COP provisions in the Cybersecurity Act, 2020 (Act 1038) for 83,293 students in 50 Senior High Schools across the Ashanti and Northern Regions of Ghana.
- Publication and issuance of COP advisories on CSA social media platforms, radio and television.
- Development of COP guidelines for children, parents, and educators on age-appropriate content.

International Cooperation

Pursuant to section 83 of the Cybersecurity Act, 2020 (Act 1038), the Authority carried out several international cooperation activities in 2023. These include:

- Facilitation of Ghana’s representation on the Freedom Online Coalition (FOC), chairing the Coalition’s Task Force on Digital Equality (TFDE) and leading projects such as the Task Force’s partnership with the Duke University Applied Ethics+ team on "Developing Inclusive and Transnational Digital Equality" and the ''Internet for All' project.
- Facilitating Ghana’s signing of the Second Additional Protocol to the Convention on Cybercrime (Budapest Convention) on Enhanced Co-operation and Disclosure of Electronic Evidence, led by the sector minister. Under the Global Action on Cybercrime Extended (GLACY+).
- Facilitating the Introductory Course on Cybercrime and Electronic Evidence for Judges and Prosecutors in Tamale and two other regions in Ghana.
- Participation in the United Nations Ad hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes and in the United Nations Open-Ended Working Group on the Security of and in the Use of ICTs and contributed to the drafting of its Annual Progress Report (APR).
- Collaboration with the Global Forum on Cyber Expertise (GFCE), the Cyber Peace Institute, the World Bank, and the World Economic fo to host the inaugural Global Conference on Cyber Capacity Building (GC3B) on behalf of Ghana. Additionally, the CSA assisted in hosting the annual GFCE meeting in Ghana.
- Facilitating the implementation of the Memoranda of Understanding signed between the CSA, the National Cyber Security Authority of Rwanda and the National Institute of Information and Communication Technologies of Mozambique.
- Partnering with the Ministry of Foreign Affairs and Regional Integration and the Ministry of Information to host a seminar on the ‘Negative Impact of

Digitalisation on Electoral Integrity, Peace and Security in Africa' as part of the International Institute for Democracy and Electoral Assistance for 2023.

Finance & Administration Initiatives

The Authority through these functional areas implemented several key initiatives in relation to its mandate. These include:

- Regularisation of Staff to support the CSA in delivering its mandate. The CSA successfully enrolled staff onto the government payroll.
- Development of conditions of service as part of drafting the Legislative Instrument for the CSA.
- Identification and development of IGF sour ces. The Ministry of Finance has been engaged in the development of IGF pending Parliamentary approval pursuant to section 23 of Act 1038.
- Establishment of the Audit Committee pursuant to section 86 of the Public Financial Management (PFM) Act, 2019 (Act 921). This is to ensure compliance with audit activities and procedures prescribed in (Act 921).
- Coordinating the production of the 2022 annual Financial Statements for Auditors' opinion and sign-off.
- Facilitating the process to ensure single source approval by the Public Procurement Authority (PPA) Board for the engagement of a consultant for the development of L.I for the CSA.
- Coordinating and Compiling the Fixed Asset Register pursuant to section 154 to 156 of the Public Financial Management (PFM) Regulation, 2019 (L.I. 2378).

Summary Of Financial Results

The Board approved Forty Million Six Hundred and Thirty-One Thousand Nine Hundred and Eighty-Nine Ghana Cedis Thirty Pesewas (GHS 40,631,989.30) for the year 2023. Nevertheless, a total of Twenty-Two Million Five Hundred and Fifty-Eight Thousand, Nine Hundred and Seventy-Five Cedis Fifty-Five Pesewas (22,558,975.55) was released to the Authority. This resulted in a shortfall of Eighteen Million and Seventy-Three Thousand and Thirteen Ghana Cedis and Seventy-Five Pesewas (GHS18,073,013.75).

The total allocation from Central GoG was Nine Million Two-Hundred Ninety-Nine Thousand Forty-Seven Cedis and Two Pesewas (GHS 9,299,047.02). Nevertheless, a release of Eight Million, Four Hundred and Seventy-Nine Thousand and Sixty-Two Cedis Two Pesewas (GHS8,479,062.02) was made to the Authority. The actual amount accessed was Six Million, Eight Hundred and Thirty-One Thousand One Hundred and Fifteen Cedis and Thirty-Seven Pesewas (GHS 6, 831,115.37). The variance of (GHS1,647,946.65) could not be accessed because the Authority was unable to meet some requirements relating to the Rayzone Project and the timing of approval for extension of the financial clearance for staff and Tier 2 contributions.

The Cyber Security Authority could not implement the Internally Generated Funds (IGF) for 2023 due to the timing of the passage of the Fees & Charges (Miscellaneous Provision) Regulations, 2023 (L. I. 2481).

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 and National Cyber Security Awareness Month (NCSAM 2022) Partners/ Sponsors for the 2023 financial year.

Management Letter/ Audit Report

The Financial Accounts of the Cyber Security Authority for the period January 2023 to December 2023 is yet to be audited in accordance with Article 187(2) of the 1992 Constitution and section 11(1) of the Audit Service Act, 200 (Act 584).

2024 Outlook Of The Authority

The following objectives underpin the CSA's programme of activities and action plan for the year 2024:

Governance Structure for Effective Operations & Administration of the Authority

Under this objective, the CSA will ensure that the necessary governance structures and policies are implemented to facilitate the effective operations and Administration of the Authority. The CSA needs to achieve this objective by implementing the Conditions of Service that has been passed by the Parliament of Ghana, and the various policies based on the directions of the Governing Board. The CSA will continue to implement good practices to achieve the mandate of the Authority.

Human Resource Capacity Development of the Cyber Security Authority

To establish and operate a world-class institution in line with the short to medium-term vision of the Authority, the CSA has taken steps to develop the human resource capacity with the needed competence and mindset to carry out its mandate to build a secure and resilient digital Ghana.

Key activities undertaken include the implementation of appropriate conditions of service for staff, the development of Standard Operating Procedures (SOP) in the various functional areas, the development of a Performance Management System, training and certification programmes for staff, and facilitating international exchanges, mentorship and coaching programmes for management-level staff of the Authority.

Regulatory Interventions

As a regulatory body, it is imperative that the Cyber Security Authority implements critical regulatory directives consistent with its mandate as outlined in the Cybersecurity Act, 2020 (Act 1038). In line with this objective for 2024, the CSA has identified critical areas of intervention in this area and will seek the necessary approvals from the Governing Board for implementation.

The CSA intends to work closely with relevant agencies including members of the Joint Cybersecurity Committee (JCC) to implement relevant regulatory measures as part of our activities in 2024. Some of the key priority regulatory areas are:

- **Continuous implementation of the Guidelines for the Licensing of Cybersecurity Service Providers, Accreditation of Cybersecurity Establishments and Accreditation of Cybersecurity Professionals** – To operationalise sections 49 to 59 of the Cybersecurity Act, 2020 (Act 1038), the CSA has developed these regulatory interventions to serve as an implementation guide for the licensing of CSPs and accreditation of CEs and CPs. The CSA will continue to implement these Guidelines to ensure that they offer their services in accordance with standards in line with domestic requirements and international best practices.
- **Implementation 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 this framework to serve as an implementation guide for the accreditation of Sectoral CERTs. The framework once finalised, will be implemented effective January 2024.
- **Development of sector-specific Directives for Sectoral CERTs** - Under section 43(2) of Act 1038 and for the effective implementation of the sectoral CERT Accreditation framework, the CSA will engage with the sectoral CERT constituents and relevant stakeholders to develop sector-specific directives on CERT operations that would reflect and address their peculiar needs, requirements and expectations of their mandate as frontline incident responders and coordinators within their sectors.
- **CII Compliance and Audit Activities** – Pursuant to section 38 of Act 1038, the Authority is expected to carry out periodic audits and inspections of CIIs to ensure compliance with the provisions of Act 1038 and the Directive for the Protection of CII. Additionally, the CIIP unit shall develop Frameworks for Risk Assessment, Risk Management, Crisis Management and Audit, Compliance and Monitoring of CIIs.

Sustainable Funding for Ghana's Cybersecurity Development

Per sections 29 to 34 of the Cybersecurity Act, 2020 (Act 1038), a Cybersecurity Fund is expected to be established to provide guaranteed funding for the country's cybersecurity development and protect Ghana's investment in digital transformation. Sustained funding is required to implement (Act 1038) and the National Cybersecurity Policy & Strategy. Therefore, the CSA, working under the direction of the sector minister and the Governing Board will continue to work closely with the Ministry of Finance and other relevant institutions to operationalise the above provisions in (Act 1038).

Implementation of Priority Cybersecurity Initiatives

Since its establishment, the CSA has implemented a number of critical interventions to consolidate Ghana's formative cybersecurity development. The CSA will continue to implement these initiatives in 2024. Some of these critical initiatives include:

- The implementation of the Safer Digital Ghana campaign
- The implementation of COP frameworks to protect children online
- The implementation of the Rayzone Project
- Development of the CERT ecosystem
- International cooperation activities to improve Ghana's response to cybersecurity incidents.

Operationalising Approved Organogram for the CSA

The approved organisational structure illustrates the organisational design and Human Resource Plan in accordance with the Public Services Commission standards. The structure has been developed in a manner that is consistent with the mandates and priorities of the CSA. The design will be operationalised to ensure structural stability, optimal layering and appropriate span of control, considering current and future operational requirements.

Functional Areas Key Initiatives for 2024

Apart from their day-to-day operational functions, the following are highlights of key programmes and activities to be implemented by the functional areas of the Authority:

National CERT (CERT-GH)

- Monthly reporting of the State of Cybersecurity in Ghana.
- Operationalisation of Ghana's membership of AfricaCERT and the Forum of Incident Response and Security Teams (FIRST).
- Deployment of an Information Sharing Platform for the various Sectoral CERTs.
- Implementation of Accreditation of Sectoral CERTs (Registration of CERT Constituents) in collaboration with the Legal and Compliance Division.
- Implementation of Incident Reporting by Licensed/Accredited CSPs/CEs/CPs
- Implementation of MoU/Information Sharing on Incidents/Threats with Bank of Ghana's Financial Industry Command Security Operations Centre (FICSOC).
- Conduct Cybersecurity Exercises for CII Owners (in collaboration with the Critical Information Infrastructure Protection Division).
- Develop and update the Division's Standard Operating Procedures (SOP).

Critical Information Infrastructure Protection (CIIP)

- Registration of all Designated CIIs
- Implementation of Audit and Compliance programmes using the Directive for the Protection of Critical Information Infrastructure.
- Coordinate the development and implementation of a Risk Management Framework for designated CIIs and GDIs.
- Coordinate the development and implementation of a Crisis Management Framework for designated CIIs.
- Coordinate the development and implementation of an Audit, Compliance and Monitoring Framework for designated CIIs.
- Coordinate the development of Sectoral Directives for key CII sectors including the Government Sector, Energy Sector; Health Sector; the Banking and Finance Sector and the Information and

Communication Technology Sector.
- Analyse to identify potential institutions which qualify as CII Owners for the attention of the sector minister for possible designation pursuant to section 35 of Act 1038.
- Capacity Building programmes including training for designated CII Owners.

Capacity Building & Awareness Creation (CBAC)

- Implement capacity-building and awareness-creation programmes throughout the year in collaboration with relevant JCC members and other governmental institutions as well as other non-governmental actors.
- Conduct cybersecurity awareness programs in all 270 districts/constituencies of Ghana, with a specific emphasis on community engagement and collaboration with the District Security Councils through the various District Co-ordinating councils.
- Raise awareness, with a special focus on the unique requirements of people with disabilities.
- Leverage collaborations with global partners such as the Council of Europe in the implementation of Global Action on Cybercrime Enhanced (GLACY-E), and the Technical Assistance and Information Exchange instrument of the European Commission (TAIEX) to further enhance the capacity of the Criminal Justice Sector.
- Organise the 2024 edition of the National Cyber Security Awareness Month (NCSAM).

Child Online Protection (COP)

- Launch and implementation of the National Child Online Protection (COP) Framework.
- Awareness creation and sensitisation programmes on cyber hygiene practices and the COP-related provisions in the Cybersecurity Act, 2020 (Act 1038).
- Implementation of the National Cybersecurity Challenge programme in collaboration with COP stakeholders and partners.
- Commemoration of the Africa Safer Internet Day (ASID).
- Local cooperation and deployment of COP 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.
- Implementation of the COP components of the Legislative Instrument (L.I) of the Cybersecurity Act, 2020 (Act 1038).
- Establishment of the National Child Online Protection (COP) Taskforce.
- COP collaboration with PTAs on awareness creation across the country.

Law Enforcement Liaison Unit (LELU)

- Operational enhancement of the 24/7 Point of Contact (Article 35 of the Budapest Convention and section 83 of the Cybersecurity (Act 1038).
- Operational enhancement of forensic workstations for LELU's operations.
- Investigations and prosecutions of high-priority cases reported to the Authority through the National CERT.
- Cybersecurity incidents and intelligence analysis and reporting activities.
- Support the development & implementation of Data Retention Framework for Service Providers pursuant to section 77 of Act 1038.
- Support 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, and CID, pursuant to section 76 of Act 1038 in collaboration with Cybersecurity Technology Standards.
- Internal security of the CSA, including implementation of appropriate physical security and access control systems.
- Countering Disinformation related to Election 2024 (activities of the Joint Taskforce).
- Security Operations including overt and covert activities, due diligence relevant to Cybercrime/Cybersecurity interventions, evidence collection process as part of the investigations to secure prosecution and cyber intelligence-related activities.

Legal & Compliance (LECO)

- Coordinate the Development of a Legislative Instrument (L.I) for the Cybersecurity Act, 2020 (Act 1038).
- Implement the guidelines 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.
- Collaborate with CERT-GH and other Accredited CERTs for the development of sector specific regulatory directives for Sectoral CERTs.
- Collaborate with CIIP to develop Sectoral Directives for key CII sectors including the Government Sector, Energy Sector; Health Sector; Financial Sector and the Telecommunications Sector.
- Collaborate with CIIP in the implementation of Audit and Compliance programmes in line with the Directive for the Protection of Critical Information Infrastructure.
- Collaborate with CERT-GH in the implementation of the Framework for the Accreditation of Sectoral CERTs.

Cybersecurity Technology Standards

- Review, Audit & Establish cybersecurity specifications/recommendations for Government Digitalisation Initiatives (GDIs), working in collaboration with NITA and other JCC members.
- Development of baseline cybersecurity specifications and cybersecurity guidance on specific technology by government, children, the public, and businesses in collaboration with NITA, and other JCC members.
- Development & Implementation of Data Retention Technology Framework for Service Providers pursuant to section 77 of Act 1038 in collaboration with LELU.
- Develop technology specifications for interception capabilities for service providers, in collaboration with LELU, NCA, and other JCC members, as mandated by section 76 of Act 1038.
- Coordinate and support the development of technical proposals and guidelines for Cybersecurity programmes and projects (including the CSA's projects under GDAP, for Sectoral CERTs, etc.)
- Coordinate the implementation of the Rayzone Project.

Information Technology (IT) Services

- Implementation of a Dedicated Secured Network for CSA Operations.
- Implementation of a business continuity/backup solution for CSA's IT Systems & Resources.
- Implementation of an Active Directory to centralise the administration of computer and network devices.
- Deployment of the Digital Platform for the implementation of the National Cybersecurity Policy & Strategy.
- Implementation of Integrated Regulatory Management System (IRMS) for the CSA.
- Oversee the Implementation of an Information Classification System across the CSA's E-mail and Document Management System.
- Support the deployment of the Rayzone technology and other technologies to be deployed as part of the operations of the CSA.
- Support the development and implementation of IT Policies and Procedures to govern the use of computers, networks and IT resources of the CSA.
- Internal capacity building on IT-related issues at the CSA.
-

Joint Cybersecurity Committee (JCC) Secretariat

- Coordinate the development of JCC sub-committees & JCC meeting regulations.
- Coordinate the establishment of the Industry Forum pursuant to section 81 of Act 1038.
- Support the development of Industry Code pursuant to section 82 of Act 1038.
- Coordinate meetings of the JCC, & JCC Sub-Committee and facilitate meetings with the Industry Forum.
- Coordinate Public-Private Partnership Programmes on cybersecurity matters.
- Coordinate the adoption and implementation of the National Cybersecurity Policy and Strategy (NCPS).
- Coordinate the planning and implementation of JCC and Industry programmes and activities.

Administration

- Implement Administration related policies & procedures including:
  - Schemes of Service
  - Conditions of Service
  - HR Manual/Policy
  - Job Description (JD)
- Coordinate staff training and professional development.
- Administer staff salaries.
- 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.
- Compile Asset Register and regular inventory updates.
- Procure logistical items for the operations of the CSA.

- Coordinate procurement functions of CSA's funding under the Ghana Digital Acceleration Project (GDAP).
- Establish a Confidential Registry.
- Participate in all multilateral engagements.
- Explore bilateral engagements through courtesy calls and signing of Memoranda of Understanding (MoUs).

Finance

- Development & adoption of financial administration-related policies & procedures for consideration by the Governing Board.
  - Financial Administration Policy
  - Internal Control Policy
  - Development Partners Financial Support Policy
- Coordinate the implementation of payroll validation and payment of salaries on the Government payroll.
- Coordinate the implementation of the Ghana Integrated Financial Management System to cover Internally Generated Funds (IGF) of the CSA in accordance with Regulation 13(2) and 14 of the Public Financial Management Regulation, 2019 (L.I. 2378)
- Coordinate the establishment of the Cybersecurity Fund.
- Coordinate the implementation of financial management under the Ghana Digital Acceleration Project (GDAP)
- Finance will coordinate the implementation of Internally Generated Funds (IGF) of the CSA per section 23 of the Cybersecurity Act, 2020 (Act 1038).
- Compilation of Management and Financial Reports pursuant to section 79 of the PFM Act, 2016 (Act 921).
- Lead fundraising from development partners.
- Coordinate and source external funding for some programmes and activities of the CSA, among others.

Internal Audit

- Implementation of Audit Committee recommendation for the CSA pursuant to section 86(1) of the PFM Act, 2016 (Act 921).
- Development of Audit Plan for 2024 pursuant to section 83(4) 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).
- Quarterly and periodic audit of CSA's activities for 2024 pursuant to section 22(4) of the Cybersecurity Act, 2020 (Act 1038), among others.

Communications

- Develop and Implement a Communications Policy/Plan/Strategy for the Authority.
- Develop and Implement Corporate Protocol Policies and Procedures for the CSA.
- Coordinate Publications of the Authority (NCSAM 2024 Report, Annual Report of the CSA, etc).
- Build and maintain strong relations with the media and other strategic stakeholders.
- Develop messages consistent with the organisational strategy and corporate objectives.
- Promote the corporate brand through media engagements, public speaking engagements, corporate productions and presentations.
- Develop and implement a media plan for 2024 regulatory activities.

CORPORATE INFORMATION

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

Gallery


NAVASCO


CYBERSECURITY
CHALLENGE 2023
NATIONAL
CYBERSECURITY
CHALLENGE 2023

CYBER SECURITY AUTHORITY
FREEDOM AND JUSTICE
CSA

CYBER SECURITY AUTHORITY

www.csa.gov.gh

A SAFER DIGITAL GHANA