CYBER SECURITY AUTHORITY
(CSA)

ANNUAL REPORT

2024

www.csa.gov.gh

A SAFER DIGITAL GHANA

CYBER SECURITY AUTHORITY
FREEDOM AND JUSTICE
CSA

TABLE OF CONTENT

ACRONMYS

ACEPA	-	African Centre for Parliamentary Affairs
Africa CERT	-	Africa Computer Emergency Response Team
BoG	-	Bank of Ghana
CBAC	-	Capacity Building and Awareness Creation
CE	-	Cybersecurity Establishment
CERT-GH	-	Computer Emergency Response Team, Ghana
CII	-	Critical Information Infrastructure
CIIP	-	Critical Information Infrastructure Protection
CP	-	Cybersecurity Professional
CSP	-	Cybersecurity Service Provider
CSA	-	Cyber Security Authority
FIRST	-	Forum of Incident Response and Security Teams
GDAP	-	Ghana Digital Acceleration Project
GDI	-	Government Digitalisation Initiatives
GHCCI	-	Ghana Chamber of Construction Industry
GHS	-	Ghana Health Service
GIFMIS	-	Ghana Integrated Financial Management Information System
GTEC	-	Ghana Tertiary Education Commission
IDEG	-	Institute for Democratic Governance
IGF	-	Internally Generated Funds
ITU	-	International Telecommunication Union
JCC	-	Joint Cybersecurity Committee
LELU	-	Law Enforcement Liaison Unit
LI	-	Legislative Instrument
MFWA	-	Media Foundation for West Africa
MoU	-	Memorandum of Understanding
NCPS	-	National Cybersecurity Policy and Strategy
NCSAM	-	National Cyber Security Awareness Month
NCSC	-	National Cyber Security Centre
NCSS	-	National Cyber Security Secretariat
NIA	-	National Identification Authority
PoC	-	Point of Contact
SEI	-	Software Engineering Institute
UNICEF	-	United Nations Children's Fund
WANEP	-	West African Network for Peacebuilding

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 and promote the development of cybersecurity in the country as well as provide for related matters.

The CSA officially started operations on October 1, 2021; starting as the National Cyber Security Secretariat (NCSS) with the appointment of a National Cybersecurity Advisor in 2017 and subsequently 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

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

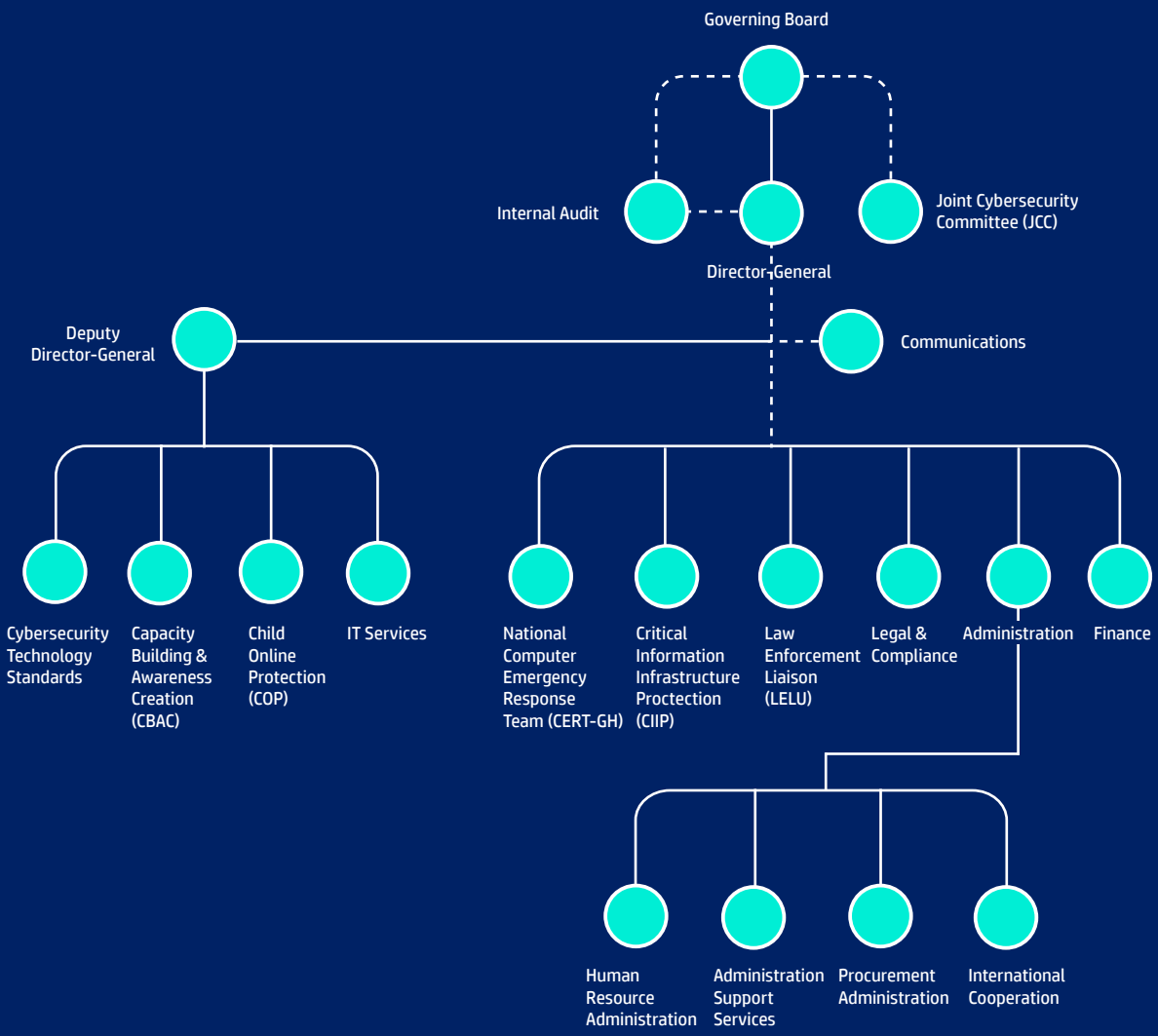
FUNCTIONS OF THE AUTHORITY

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

Advise	Government and 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 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 an oversight of government's infrastructure programmes for the ICT sector, the development of a robust framework to support the digitalisation 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 exposing women, children and persons with disabilities to 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 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 foremost 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.

His educational background includes an undergraduate degree from the University of Trento in Italy, achieved with cum laude honours. 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 several 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 several 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

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

He 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.

Mr. 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. Henry Quartey

His ministerial experience includes serving as Greater Accra Regional Minister, Deputy Minister for National Security, and Deputy Minister for the Interior.

Mr. Henry Quartey is the Minister for the Interior and the Greater Accra Regional Minister.

He holds an Executive Master of Arts Degree in Conflict, Peace and Security from the Kofi Annan International Peacekeeping Training Centre (KAIPTC) and has undertaken executive studies in National and International Security at the Harvard Kennedy School of Government in the United States of America. These academic pursuits have enhanced his strategic thinking and policy formulation capabilities.

Mr. Henry Quartey has played critical roles in Parliament and government, including as a member of the Appointments Committee and a participant in various legislative and oversight committees.

Hon. Dominic Nitiwul

Mr. 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.

He has been a Member of Parliament since 2002 and a one-time Deputy Minority Leader of 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, Appointments 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. Sackey is a Ghanaian IT expert with over twenty-five years' experience.

His 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 and Digitalisation and was a member of the then National Cyber Security Technical Working Group.

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

He holds a bachelor's degree in computer science and a master's degree in software engineering from the University of North Carolina in Charlotte, USA.

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.

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.

Amb. Mrs. Esther Dzifa Ofori

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

On leaving Multichoice, she set up a consultancy specialising in management and public relations before her appointment as the Chief Executive Officer of the Ghana Trade Fair Company (GTFC).

Her role at the GTFC 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 imported foreign goods. She was trained in public relations, executive communications skills and human resource development.

In 2017 she 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 programme for the people of Equatorial Guinea to study English in Ghana rather than in Nigeria and the United Kingdom. Through the years, she has been a television presenter for Women's Digest, a 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
- Madam Mercy Araba Kertson
  Director, Administration
- Mr. Alexander Oppong
  Director, Capacity Building and Awareness Creation
- Mr. Benjamin Ofori
  Head, Critical Information Infrastructure Protection Unit
- Lt. Col. George Eduah Beesi
  Head, Law Enforcement and Liaison Unit
- Mr. Johnson Awua
  Chief Accountant/ Head, Finance
- Mr. Stephen Cudjoe-Seshie
  Head, Computer Emergency Response Team

Introduction

As the Chairperson of the Governing Board of the CSA, it is a privilege to present this comprehensive report, which reflects the remarkable achievements and progress made by the Authority in 2024. This year has marked a significant period in strengthening Ghana's cybersecurity ecosystem, and the CSA has been pivotal in driving initiatives that ensure a secure and resilient digital environment for all Ghanaians.

The work of the CSA is integral to the Government of Ghana's broader vision of a digitally inclusive and resilient economy. With the increasing reliance on digital technologies, cybersecurity is paramount in safeguarding critical infrastructure, protecting the privacy of citizens, and ensuring the smooth operation of businesses and government services. This report highlights the CSA's role in advancing these objectives while contributing to the overarching digital transformation agenda.

REPORT

By Chairperson of the Governing Board

Key Achievements in 2024

In 2024, the CSA made significant strides in its mission to enhance the cybersecurity landscape of Ghana. One of the most notable achievements was the adoption of the revised National Cybersecurity Policy and Strategy (NCPS), which provides a comprehensive framework for addressing emerging cyber threats. The updated strategy when implemented will strengthen the country's capacity to tackle cybercrime, protect national assets, and ensure a resilient digital economy. Additionally, the cybersecurity regulations, developed to support the operationalisation of the Cybersecurity Act, 2020 (Act 1038), were submitted to Parliament for approval. The regulations represent a crucial step towards the formal enforcement of cybersecurity laws and the establishment of stronger oversight mechanisms for cybersecurity activities.

Another major milestone for the CSA in 2024 was the launch of the Child Online Protection (COP) Framework aimed at tackling incidents of Child Online Sexual Exploitation and Abuse including child sexual abuse material, online harassment, and cyberbullying against children. The document is part of efforts to create safer online spaces for children, helping to mitigate risks such as cyberbullying, exploitation, and exposure to harmful content. It entails a combination of legal, educational, and technological measures to ensure that the digital experience of minors is secure and protected.

In recognition of its considerable progress in strengthening cybersecurity, Ghana was ranked as a Tier 1 country on the Global Cybersecurity Index (GCI) by the International Telecommunication Union (ITU) in 2024. This achievement highlights Ghana's commitment to building a robust cybersecurity framework, enhancing its legal and regulatory environment, and fostering international collaboration. Tier 1 ranking reflects the country's strategic investments in cybersecurity infrastructure, capacity building, and its efforts to ensure the protection of citizens and businesses against cyber threats. Ghana's position on the GCI demonstrates its leadership in the region and sets a sturdy foundation for continued growth and innovation in cybersecurity.

As a regulator, the CSA has made progress in regulating the cybersecurity sector in Ghana. More than One Thousand, Five Hundred and Sixty-Three (1,563) CPs,Two Hundred and Seventy-Six (276) CSPs, and Seventy-Three (73) CEs were registered, reflecting a strengthened effort to raise the standards of the sector.

The CSA's efforts to promote cybersecurity awareness and build capacity nationwide were also noteworthy. Through various public engagement initiatives, including the National Cyber Security Awareness Month (NCSAM) 2024, the Authority was able to sensitise over 2.1 million citizens on the importance of digital safety. More than 936,000 individuals participated in events organised nationwide as part of NCSAM, which included training and awareness campaigns targeting both the public and key sectors such as healthcare, government, and local businesses. These efforts are essential in fostering a culture of cybersecurity within the general public.

The protection of Critical Information Infrastructure (CII) remained a top priority for the CSA. In 2024, audits were conducted for six(6) key institutions responsible for managing Ghana's digital infrastructure, focusing on their compliance with national cybersecurity standards. The CSA also saw a significant increase in the registration of CIIs, with the compliance rate rising from 65% in 2023 to 79% in 2024. This improvement demonstrates the growing commitment from national institutions to adhere to cybersecurity regulations.

Outlook for 2025

As we look ahead to 2025, the CSA will continue to build on the significant achievements of 2024. The Authority remains committed to strengthening the country's cybersecurity landscape and achieving the strategic goals outlined in the Cybersecurity Act, 2020 (Act 1038). Key priorities for the Authority in the coming year will include the relaying of the Cybersecurity Regulations and the Cybersecurity (Terms and Conditions of Service) in Parliament, which will provide a clearer regulatory framework for all stakeholders and ensure consistent enforcement of cybersecurity standards

and also promote the retention of staff of the Authority. The CSA will also intensify its efforts to expand public awareness initiatives, particularly through district-level sensitisation programmes, to ensure that the public, including vulnerable groups, are adequately informed about online safety.

In addition, the CSA will advance efforts in protecting Critical Information Infrastructure by conducting regular audits, expanding compliance monitoring, and implementing sector-specific directives for industries such as healthcare, finance, and telecommunications. The Authority will advocate for the operationalisation of the Cybersecurity Fund, which will be critical in supporting its initiatives and addressing funding gaps that hinder the full implementation of its mandate.

As global cyber threats evolve, the CSA will continue to place strong emphasis on strengthening international partnerships and collaborations, engaging with international bodies and stakeholders to share knowledge, collaborate on cyber threat intelligence, and enhance Ghana's cybersecurity capabilities.

Acknowledgements

The success of the CSA in 2024 is a collective achievement, made possible through the tireless efforts of numerous individuals and organisations. I would like to express my sincere gratitude to His Excellency, the President Nana Addo Dankwa Akufo-Addo and Vice President Alhaji Dr. Mahamudu Bawumia for their unwavering commitment to Ghana's digital transformation agenda. Their leadership has been instrumental in ensuring that cybersecurity remains a key priority for the nation.

I would also like to commend Dr. Albert Antwi-Boasiako, the Director-General of the CSA, for his visionary leadership and outstanding contributions to the advancement of Ghana's cybersecurity agenda. My appreciation goes to the members of the Governing Board of the CSA, whose strategic oversight and guidance have been crucial in the Authority's growth and success.

To the management and staff of the CSA, your dedication and professionalism have played a pivotal role in achieving these remarkable results. Lastly, I would like to acknowledge the ongoing collaboration with our partners, including UNICEF, the World Bank, other international partners, civil society organisations and the media, whose contributions continue to strengthen Ghana's cybersecurity framework.

As we move forward, the CSA will work tirelessly to ensure that Ghana remains a beacon of cybersecurity excellence in Africa and beyond.

Hon. Mrs. Ursula Owusu-Ekuful
Chairperson, Governing Board
Cyber Security Authority
December 2024

Introduction

The CSA has made remarkable progress in 2024 in its mission to secure Ghana's digital ecosystem. Guided by the Cybersecurity Act, 2020 (Act 1038), our focus has been on implementing impactful regulatory frameworks, strengthening stakeholder capacity, and fostering international cooperation to build a secure and resilient digital economy. This report highlights the accomplishments of the year, the challenges encountered, and our strategic direction for the future.

REPORT

By Director-General

National Computer Emergency Response Team (CERT-GH)

CERT-GH played a critical role in safeguarding Ghana's cyber ecosystem by detecting, responding to, and mitigating cybersecurity incidents. In 2024, it operationalised a real-time information-sharing platform integrating feeds from AfricaCERT and local entities, developed an accreditation framework to enhance Sectoral CERT capabilities, and published a comprehensive mid-year cybersecurity report to guide national policy and resource allocation.

Critical Information Infrastructure Protection (CIIP)

Efforts to secure Ghana's critical digital infrastructure resulted in a rise in CII registration compliance from 65% in 2023 to 79% in 2024. Compliance audits were conducted for six key institutions, sector-specific directives were drafted, and a database for 69 Government Digitalisation Initiatives (GDIs) was established.

Law Enforcement Liason

As part of efforts to enforce Cybersecurity measures, the CSA investigated 155 cyber-related cases, leading to the recovery of GHS 49.6 million in financial losses. Two forensic workstations were established for advanced digital investigations, and law enforcement agencies were provided with weekly intelligence updates to strengthen security coordination.

Legal and Compliance (LECO)

As part of efforts to increase compliance for the licensing and accreditation regime, which commenced in 2023, the CSA continued to engage stakeholders on the process and provided direct assistance to those who needed help to complete their application processes. The CSA successfully registered a total number of Two Hundred and Seventy-Six (276) CSPs, Seventy-Three (73) CEs and One Thousand, Five Hundred and Sixty-Three (1,563) CPs.

Administration and Finance

Despite financial constraints, 37.94% of the approved budget was released to support the operations of the Authority. The Ghana Digital Acceleration Project (GDAP) was implemented to support digital transformation initiatives of the Authority. Advocacy efforts were also intensified to secure full retention of Internally Generated Funds (IGF) to enhance the operational funds of the institution.

Challenges

While 2024 marked significant progress, a major challenge which affected the smooth operation of the institution was funding constraints.

The way forward

The accomplishments of 2024 are a testament to the dedication of the CSA team, our partners, and stakeholders. As we look ahead to 2025, our priorities include the implementation of the Cybersecurity Regulations, strengthening district-level outreach, and enhancing Ghana's resilience against emerging cyber threats. Together, we will continue to secure Ghana's digital future and solidify our position as a leader in Africa's cybersecurity landscape.

Acknowledgement

I extend my heartfelt appreciation to our stakeholders, the Governing Board of the CSA, and our dedicated staff for their steadfast support and commitment. Your contributions have been pivotal to our progress. I look forward to continued collaboration as we work towards a more secure and resilient digital landscape for all.

Dr. Albert Antwi-Boasiako
Director-General
Cyber Security Authority
December 2024

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 Committee
- Technical Committee

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; coordinating 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) UNIT

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 compliance Audit of CII, in adherence to the cybersecurity Act and the Directive for the protection of CIIs, 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 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.

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)

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 in 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, 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 functional area plays an oversight role for the 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 at the CSA plays a vital role in managing external relations and corporate affairs. It works collaboratively across all functional areas to design and implement effective communication strategies that support the organisation's objectives. The unit leads the development and promotion of the CSA's corporate brand through stakeholder engagement, strategic messaging, and visual representation. By ensuring consistent and impactful communication, the unit enhances the CSA's visibility, strengthens stakeholder trust, and supports the organisation's mission and values.

OVERVIEW OF 2024 OPERATIONAL PERFORMANCE

The operations of the Authority in the year under review were guided by strategic goals set by the Board and Management in accordance with the Authority's core mandate as specified in the Cybersecurity Act, 2020 (Act 1038).

ADMINISTRATION

Human Resource

In 2024, the Governing Board of the CSA, chaired by Mrs. Ursula Owusu-Ekuful, who also serves as Minister for Communications and Digitalisation, played a crucial role in developing Cybersecurity Regulations and the Conditions of Service. During the reporting year, relationships with other public service institutions were strengthened, and this fostered human resource support from these institutions, including officers on secondment to complement the staffing capacity of the Authority. Additionally, following the staff regularisation, a performance appraisal instrument was developed and approved. The Human Resources functional area coordinated the conduct of performance appraisal for all eligible staff. Towards the end of the year, Management successfully negotiated a 20% salary increase for staff, which is to be implemented effective next year.

Workforce Planning, Staff Turnover and Retention

During the reporting year, the Authority recruited eight staff after securing financial clearance from the Ministry of Finance to achieve the mandate of the Authority. As of December 2024, a total of ninety-seven personnel were regularised as staff of the Cyber Security Authority.

In the course of the year, a total of fourteen staff (7 males and 7 females) exited from the Authority. The primary reason for the separations was the pursuit of further studies. In addition, two seconded officers completed their term of service with the Authority.

The workforce composition as at December 31, 2024, is as follows

Gender	Male	Female	Total
Regularised	57	40	97
Secondment	6	4	10
Contract/ Consultants	6	0	6
National Service	0	0	0
Total	69	44	113
(%)	61.06%	38.94%	100

Staff Training and Development

The CSA believes that training and development is fundamental to staff performance and for that reason, based on 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 recruited eight(8) staff, there was a total of ninety-seven staff on the Government of Ghana payroll system, all the ninety-seven staff were paid through the Integrated Personnel Payroll Database (IPPD). Secondment officers continued to draw their salaries from the mother organisation while the Authority paid approved allowances due to them. Contract staff were paid through government subventions whilst consultants were paid through the e-Transform/GDAP (World Bank) Project.

24-Hour Shift System

Pursuant to Section 48(1) the Authority is mandated to establish a cybersecurity incident point of contact to facilitate reporting of a cybersecurity incidents by the general public is operational. 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.

Legal and Compliance

Implementation of Guidelines for the Licensing of Cybersecurity Service Providers (CSPs), Accreditation of Cybersecurity Establishments (CEs), and Accreditation of Cybersecurity Professionals (CPs)

With the implementation of the guidelines for the licensing of CSPs, accreditation of CEs, and accreditation of CPs, the CSA had a target to register a total of One Hundred (100) CSPs, Fifty (50) CEs, and One Thousand (1,000) CPs. As of December 2024, the target had been exceeded, as a total of Two Hundred and Seventy-Six (276) CSPs, Seventy-Three (73) CEs, and One Thousand, Five Hundred and Sixty-Three (1,563) CPs had been registered with the Authority.

Inauguration of Independent Assessors

As part of its regulatory processes, the CSA recognised the need for Independent Assessors to support the execution of key regulatory activities in accordance with Act 1038 and other relevant laws of Ghana. These activities include the inspection of Cybersecurity Establishments and conduct cybersecurity audits of relevant institutions.

On October 22, 2024, eighteen(18) Independent Assessors were successfully inaugurated to support the CSA in conducting site inspections, cybersecurity audits, research, and development programs, and in providing regular reports on activities performed.

Through this mechanism, the CSA seeks to foster collaboration with Cybersecurity Professionals while enhancing their visibility and contribution within the regulatory framework.

Implementation of strategies to ensure full compliance with the Guidelines

To ensure compliance with technical and operational standards, the CSA conducted inspections of Security Operations Centers (SOCs) and Digital Forensics Service Facilities of Cybersecurity Establishments applying for accreditation.

In June 2024, as part of the processes for issuing final certificates of accreditation for Cybersecurity Establishments, the CSA conducted inspections and physical assessments of the technology setups and technical processes of eighteen 18 establishments.

This contributes to strengthening the integrity and effectiveness of Ghana's cybersecurity regulatory framework.

Furthermore, the CSA has commenced enforcement activities to compel non-compliant constituents to submit complete applications as part of the licensing and accreditation process. To this end, the CSA has commenced the issuance of regulatory notices to defaulting constituents, directing them to comply with relevant directives within a stipulated timeframe determined by the Authority. Accordingly, a total number of One Hundred and Forty-Five (145) regulatory notices have been sent to defaulting constituents, compelling them to comply with the Guidelines.

Development of Legislative Instrument for the Cybersecurity Act, 2020 (Act 1038)

To give true meaning to the provisions of the Act, the CSA collaborated with the Office of the Attorney-General and Ministry of Justice and key stakeholders to develop regulations to support the implementation of the Cybersecurity Act, 2020 (Act 1038).

Two drafts, the Legislative instrument for the Cybersecurity Act, 2020 (Act 1038), and the Regulations on Conditions of Service for staff of the Authority, were laid in parliament on September 3, 2024. The documents seek to establish clear guidelines and standards for cybersecurity practices, aligning with international best practices and benchmarks in Ghana and to provide the legal framework needed to effectively implement the provisions of Act 1038 and to strengthen cybersecurity governance in Ghana. The Legislative instrument, however, did not mature before the end of the 8th parliament.

Capacity Building and Awareness Creation

The CSA in 2024 set out to enhance the cyber knowledge and skills of various stakeholders, including Children, the Public, Businesses and Government agencies. Key initiatives included monthly advisory/alerts to the public (in collaboration with CERT-GH), social media cybersecurity awareness creation, cybersecurity awareness and best practices sessions for Ministries, Regional/District level (Selected Districts/Constituencies) cybersecurity awareness creation, and the implementation of the NCSAM 2024.

Other notable activities included the development of a cyber hygiene curriculum for the Ghana Chamber of Construction Industry (GHCCI), aimed at improving cybersecurity awareness and practices within the construction sector; and a cyber hygiene module also developed and successfully facilitated for healthcare personnel, enhancing their ability to manage cybersecurity risks in healthcare.

The following are some of the capacity building and awareness creation activities undertaken during the year:

National Cyber Security Awareness Month (NCSAM) 2024: The CSA has organised the National Cyber Security Awareness Month (NCSAM) since 2018 to safeguard Ghana's digital landscape and promote cybersecurity awareness. In 2024, with democracies worldwide grappling with the challenges of digital information manipulation that undermine democratic processes, the CSA organised the NCSAM under the theme: ***"Combating Misinformation/Disinformation in a Digitally Resilient Democracy—Our Collective Responsibility."*** The initiative aimed to build citizens' capacities to detect and prevent misinformation, safeguarding national security and democratic integrity. The 2024 NCSAM was characterised by extensive partnerships with civil society organisations

(CSOs) to facilitate cybercrime and cybersecurity sensitisation engagements. These collaborations heightened awareness and built capacity on the dangers of misinformation and disinformation among diverse groups. By the end of the 2024 edition, 936,235 individuals had been sensitised, significantly raising awareness of cybersecurity risks and best practices.

Public In-person Engagements: A total of 60,377 individuals were sensitised through cybersecurity workshops and forums, a significant increase from the 2,975 reached in 2023. Key groups engaged included CAMFED trainers, Digital Champions Summit participants, members of the Insurance Brokers Association of Ghana, district assemblies, and various colleges and universities.

Cyber Hygiene Programme/Government Cybersecurity Champions Awareness Programme: The Ministry of Information, consisting of 20 staff members, participated in the cyber hygiene program during the third quarter of 2024. Additionally, 50 IT heads and health administrators attended specialised workshops aimed at improving cybersecurity compliance.

Social media and Radio Engagements: Public was sensitised on different issues through social media and traditional media engagements for enhanced cybersecurity best practices.

The CSA held Initial discussions with GTEC to develop a cybersecurity qualification and competency framework aimed at regulating educators and institutions in this field.

The CSA collaborated with the Ghana Health Service to develop and deliver tailored cybersecurity training programs to over 1,000 healthcare professionals through the e-learning lessons hosted on the GHS platform.

Critical Information Infrastructure Protection

Registration of Critical Information Infrastructures (CII)

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

- 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

At the end of the year, the following milestones were achieved:

Issuance of Certificate for Registration	Current Update
Nomination of CII Point of Contact	93% of CII Owners have submitted their POC nominees.
Completion and submission of CII Registration Form	72% of CII POCs have submitted their completed forms to the CSA.
Issuance of Certificate for Registration	35% of CII Owners have been issued with certificates of registration

Risk Management and Audit, Compliance, and Monitoring Framework/Programme for CIIs

To ensure collaboration and cooperation with CII Sectors and adoption of the Risk Assessment Framework, the Authority organised workshops with industry experts in CII Sectors (Banking & Finance, Education, Emergency, Energy, Food & Agriculture, Government, Health, ICT, Manufacturing, Mining, and Transport) to solicit input on the pertinent risks and the current processes used in managing risks in the respective sectors. The draft framework which is currently under review will strengthen mechanisms to ensure compliance with the Directive for the Protection of CIIs and the Cybersecurity Act, 2020 (Act 1038).

Additionally, the CSA conducted audits on six institutions responsible for government digitalisation projects. Audit reports have been submitted for remediation to enhance compliance with cybersecurity standards and improved protection for government digitalisation projects.

Identification and Registration of Government Digitalisation Initiatives (GDIs)

A database of sixty-nine (69) GDIs has been developed and is currently undergoing review. This database will provide the CSA with a comprehensive overview of GDIs requiring protection, ensuring focused efforts on securing digitalisation initiatives.

Computer Emergency Response Team

Activation of Computer Emergency Response Team (CERT) Information Sharing Platform

The CSA fully operationalised an information-sharing platform to support stakeholders in the CERT ecosystem for real-time communication and collaboration. In November 2024, the information-sharing platform went live, with a feed from AfricaCERT successfully enabled.

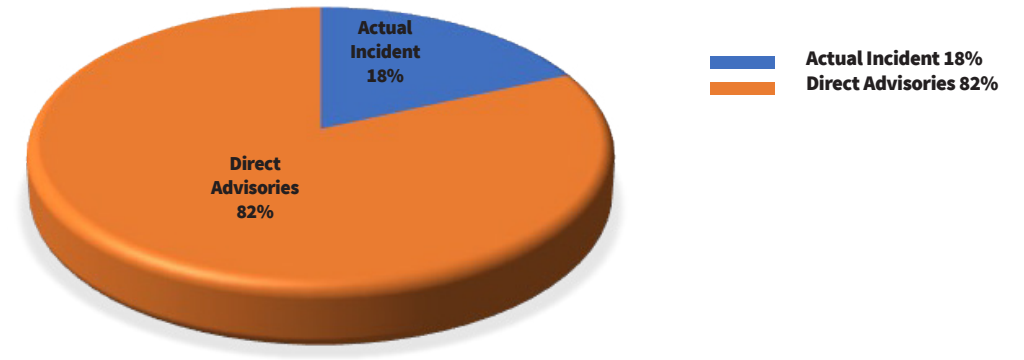
Accreditation of Sectoral Computer Emergency Response Teams (CERTs)

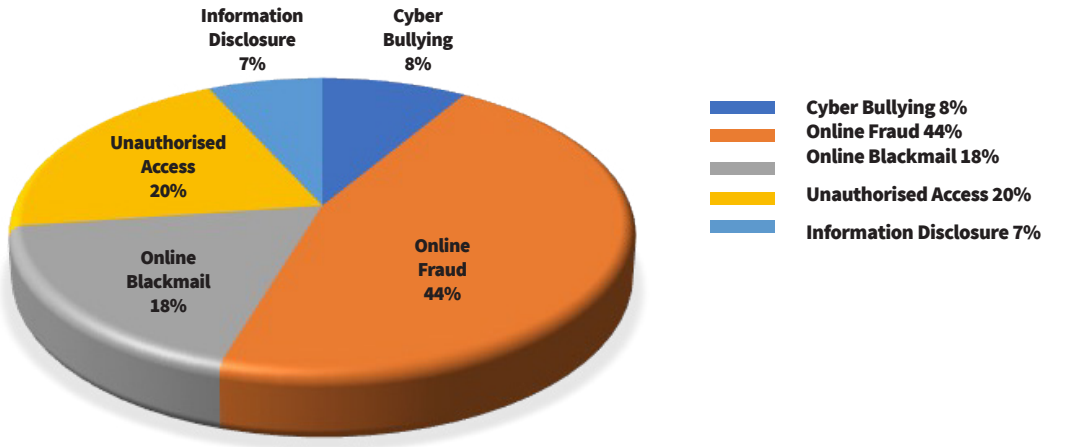
Pursuant to section 44(4) of the Cybersecurity Act, 2020 (Act 1038) which mandates the CSA to accredit and oversee the operations of Sectoral CERTs, the CSA has developed draft guidelines for the accreditation of Sectoral CERTs to ensure oversight supervision of the operations of the Sectoral CERTs and compliance with incident reporting obligations across the various sectors. A draft gazette outlining the accreditation framework has been developed to provide a clear roadmap for implementation. Additionally, a notice of designation has been successfully issued to the Bank of Ghana to commence the implementation process.

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

From January 2024 to December 2024, a total of 15,146 contacts were made with the CSA through the established Points of Contact (PoC). Out of this, 2,751 (18%) were categorised as actual incidents and 12,395 (82%) were direct advisories issued to individuals and institutions to prevent them from falling victim to cybercrimes. A total of GHS23,334,662 was lost to cybercrimes based on the reports received.

Top reported incidents include online fraud, online blackmail, unauthorised access, information disclosure and cyberbullying.





Other CERT related activities implemented by the Authority include;

- Drafting a framework document to guide Incident Reporting by Licensed/Accredited CSPs/CEs/CPs in alignment with regulatory requirements.
- Operationalisation of Ghana's membership in Africa CERT, FIRST, and other International Technical Partnership by participating in online training programmes hosted by Asia Pacific CERT, Africa CERT, and the International Telecommunications Union. Ghana also hosted the 2024 ITU Regional Cyber Drill event in September, bringing together key stakeholders to address regional cybersecurity challenges.
- Facilitated engagement with the Cyber Incident Planning and Coordination Program (CIPP) and FIRST
- to design an execute cybersecurity exercises for Critical Information Infrastructure (CII) Owners.
- Production of "the State of Cybersecurity in Ghana" Report that provide both national and international insights into cybersecurity developments, trends, and challenges.
- The National CERT facilitated a cyber drill among stakeholders within the incident response ecosystem including sectoral CERTs and media. The drill focused on election related incidents (misinformation and disinformation) to prepare participants in responding and managing election related incidents.
- From January to December 2024, thirteen (13) monthly public alerts and three (3) technical alerts were released.

S/N	Month	Description of Alert
1	January	Job Scams on the Rise
2	February	Valentine's Day Scams
3	March	Surge in Online Blackmail/ Extortion Cases
4	April	Easter and Eid al-Fitr Season Scams
5	May	Surge in WhatsApp Account Takeovers
6	June	• Resurgence in Cyberbullying by Digital Lending Mobile Application Owners • Malicious Backdoor Identified in Linux Compression Library • New PHP vulnerability exposes Windows servers to remote code execution
7	July	• Online Blackmail/Sextortion Cases on the Rise
8	September	• Malicious Data Harvesting Links – Fake Account Violation Notifications • Malicious Data Harvesting Links – Fake SIM Registration Notifications • Investment Scam on Rise
9	October	• Fraudulent USA Visa Lottery Links • Fraudulent Schemes Targeting BECE Graduate • Critical Fortinet Vulnerability Under Active Exploitation
10	November	Online Shopping Scam – Black Friday Deals
11	December	Fake Presidential Candidates Election-Related Giveaways

LAW ENFORCEMENT AND LIASON

On law enforcement, several activities, including the following were carried out:

1. Investigation of Reported Cases. A total of approximately 155 cases are under various stages of investigation, including pending and completed cases.
2. Development of draft Legislative Instrument for the Cyber Security Act, 2020
3. Ensuring Operational Enhancement of 24/7 Point of Contact (PoC)
4. Operationalisation of Digital Forensic Workstation at the CSA
5. Prosecution of High-Profile Cases to bring offenders to justice.
6. Strengthened operational coordination and response capabilities with External stakeholders such as MTN, Telecel, Airtel-Tigo, FIC, BoG, EOCO, and the Ghana Police Service.
7. Conducted Joint operations conducted on loan apps with EOCO and BoG.

INTERNATIONAL COOPERATION

United Nations Ad Hoc Committee on Cybercrime

Ghana actively participated in the concluding and reconvened concluding sessions of the United Nations Ad Hoc Committee on Cybercrime which led to the adoption of the first United Nations Convention on Cybercime and significantly contributed to shaping global cybersecurity discussions. This engagement has strengthened Ghana's international presence in cybersecurity matters and fostered key partnerships.

United Nations Open-Ended Working Group (OEWG) on ICT Security

Ghana participated in the 7th and 8th sessions of the OEWG, reinforcing its commitment to multilateral cooperation on cybersecurity. These engagements have elevated Ghana's visibility in global cybersecurity governance and fostered stronger alliances with international stakeholders. Ghana advocated on matters related to capacity building, confidence-building measures and regular institutional dialogue, among others.

Bilateral Cybersecurity Partnerships

Bilateral meetings were held with countries including Australia, Germany, Zambia, Italy, Rwanda, Morocco, the United Kingdom, Barbados, and Korea to explore collaborative opportunities in cybersecurity. Additionally, six(6) courtesy calls were coordinated with Rwanda, Turkey, Zambia, the Netherlands, Saudi Arabia, and Australia. These engagements provided valuable insights into global cybersecurity frameworks and set the stage for future collaborations.

African Network of Cybersecurity Authorities (ANCA)

As chair of ANCA, Ghana played a crucial role in drafting and reviewing the ANCA Constitution and a five-year strategic plan. These efforts aim to strengthen cybersecurity governance, expand membership beyond the current seventeen (17) countries, and establish a platform for operational exchanges and practical cooperation.

Digital Rights and Inclusion Forum (DRIF) 2024

Ghana successfully hosted the 2024 edition of DRIF at the Swiss Spirit Hotel and Suites Alisa. The forum facilitated discussions on trust and accountability, data protection, privacy, artificial intelligence, digital inclusion, and human rights. The event also featured a regional dialogue in collaboration with the Freedom Online Coalition (FOC), fostering discussions on digital governance and human rights.

30th Cybercrime Convention Committee (T-CY) Meeting

Ghana, represented by the CSA, participated in the 30th T-CY meeting in Strasbourg, France. Discussions included assessments of Article 19 of the Budapest Convention. Notably, Benin acceded to the First Protocol, while the Czech Republic and Sierra Leone signed the Second Additional Protocol.

Freedom Online Coalition (FOC) Engagement

Ghana hosted and participated in the Ghana-Netherlands FOC Regional Dialogue at DRIF 2024 and the First and Second Strategy and Coordination Meetings in Geneva. Discussions highlighted digital equality, access challenges, and the evolving digital governance landscape.

ITU-INTERPOL CyberDrill

Ghana successfully hosted the ITU-INTERPOL Africa Cyber Drill at the Kofi Annan International Peacekeeping Training Centre. This event enhanced collaboration between national Computer Incident Response Teams (CIRTs) and law enforcement agencies, improving the region's capacity to detect, respond to, and recover from cyber threats.

Implementation of Cybersecurity MOUs

Ghana, through the CSA, co-hosted a capacity-building event with Rwanda's National Cybersecurity Authority and explored study exchange programmes. Ongoing bilateral engagements continue to foster knowledge-sharing and collaboration in cybersecurity. Additionally, numerous implementation meetings have been held with Mozambique to discuss tangible outcomes in 2025.

Capacity Building through Fellowships

The CSA has actively pursued fellowship opportunities for staff to enhance their cybersecurity expertise. Since 2021, 14 officials have participated in various fellowships, with 23 officials onboarded in 2024. These programs provide valuable learning experiences and exposure to global best practices in cybersecurity.

CHILD ONLINE PROTECTION (COP)

The CSA remained committed to protecting children online through policy and operational interventions:

- **Framework Implementation:** Operationalised the National Child Online Protection Framework.
- **Stakeholder Collaboration:** Partnered with UNICEF and other institutions to develop tools and policies to protect children online.
- **Legal Support:** Assisted in the prosecution of child-related cyber offenses and provided support to victims.
- The annual National Cybersecurity Challenge was successfully held among Seventy (70) schools across the country.

STAKEHOLDER ENGAGEMENTS

Launch of Industry Forum

Through the Joint Cybersecurity Committee (JCC) Secretariat, the CSA spearheaded the establishment of the Industry Forum pursuant to section 81 of the Cybersecurity Act, 2020. The Secretariat worked closely with a nine-member facilitating committee which had been set up in this regard.

This initiative was in line with the CSA's commitment to fostering a collaborative regulatory environment and elevating Ghana's cybersecurity landscape through industry cooperation and dialogue.

Other stakeholder-related activities

The Authority held a number of engagements with different stakeholders, some of which are as follows:

1. CSA and UNICEF Ghana held a meeting with a section of industry players to discuss how industry players could engage in the development of Child Online Protection guidelines.
2. Engagements for the signing and implementation of a Memorandum of Understanding (MoU) between the CSA and the Bank of Ghana (BoG).
3. Coordinated meetings with Civil Society Organisations, cybersecurity awareness programmes organised for their Staff and key stakeholders on Mis/Disinformation as Part of NCSAM 2024.

FINANCE

The Authority implemented several key initiatives to raise the funds needed to support the implementation of its mandate. These include:

1. Facilitation of Internally Generated Fund (IGF) implementation on the Ghana Integrated Financial Management System (GIFMIS) in line with Section 25(6) of the Public Financial Management Act, 2016 (Act 921) and Regulations 13 and 14 of the PFM Regulations, 2019 (L.I. 2378).
2. Ensuring the Implementation of the Ghana Digital Acceleration Project (GDAP)

An amount of GHS 5,749,843.94 (Compensation of Employees), GHS 4,682,919.12 (Use of Goods and Services) and GHS 2,591,375.62 (Capital Expenditure) were released by the Ministry of Finance at the end of the third quarter of 2024 out of the total allocated amount of GHS 10,669,390.00, GHS 10,504,796.00 and GHS 5,000,000.00 respectively for cybersecurity related activities of the CSA. A total amount of GHS 1,251,030.00 (Internally Generated Funds) and GHS 875,440.50 (Development Partners) were released to the Authority out of the total allocated amount of GHS 7,520,040.00 and GHS 6,240,927.00, accordingly, as at the end of September 2024. The total release of GHS 15,150,609.18 represents 37.94% of the budget of GHS 39,935,113.00 submitted to the Governing Board and the MoCD to operationalise the activities of the Authority for the year 2024.

CHALLENGES AND RECOMMENDATIONS

Internally Generated Funds (IGF) Capping

The CSA, as a newly established institution, requires financial support to deliver its mandate. Despite its critical mandate in securing the digital economy, the Authority has not received the required financial allocations to deliver the most critical of its mandate. The Authority requires adequate financial resources to implement the conditions of service as part of the regularisation of 100 staff based on the Financial Clearance granted by the Ministry of Finance to retain the current staff.

Therefore, a 100% retention of the IGF is required to provide an operational lifeline to the Authority until the Cybersecurity fund is duly established pursuant to Section 29 of the Cybersecurity Act.

Non-compliance with Section 36 of Act 1038 (CII Registration)

Seven per cent (7%) of CII owners have not submitted their POC nominations to the CSA, contravening Gazette Notice No. 140 pursuant to Section 36 of Act 1038. Furthermore, 28% of the nominated CII POCs have not registered their critical systems with the CSA. Legal notices have been sent to non-compliant CII Owners. There is a need to bridge the knowledge gap on the importance of protecting CIIs to maintain Ghana's national security and the socio-economic well-being of Ghanaians.

Other major challenges the CSA faced are

- Inadequate staffing capacity
- Delay in operationalisation of the Cybersecurity Fund pursuant to section 30 of the Cybersecurity Act, 2020 (Act 1038)
- Inadequate office space and related logistical constraints
- Inadequate technical tooling

KEY INITIATIVES FOR 2025

In 2025, the CSA will continue to build on the significant achievements of 2024. The Authority remains committed to strengthening the country's cybersecurity landscape and achieving the strategic goals outlined in the Cybersecurity Act, 2020 (Act 1038).

Key priorities for the Authority will include the relaying of the Cybersecurity Regulations in Parliament, which will provide a clearer regulatory framework for all stakeholders and ensure consistent enforcement of cybersecurity standards.

The CSA will also intensify its efforts to expand public awareness initiatives, particularly through district-level sensitisation programmes, to ensure that the public,

including vulnerable groups, are adequately informed about online safety.

The Authority will advocate for the establishment of the Cybersecurity Fund, which will be critical in supporting its initiatives and addressing funding gaps that hinder the full implementation of its mandate.

As global cyber threats evolve, the CSA will continue to place strong emphasis on strengthening international partnerships and collaborations, engaging with international bodies and stakeholders to share knowledge, collaborate on cyber threat intelligence, and enhance Ghana's cybersecurity capabilities.

The CSA will further engage stakeholders for the implementation of the National Cybersecurity Policy and Strategy and the Child Online Protection Framework, which were launched in October 2024. Industry players will also be engaged working with the Industry Forum Facilitating Committee to operationalise the Industry Forum.

In the 2025 operational year, the CIIP functional area will implement specifically the following programmes/activities.

1. Registration of all designated CIIs and the implementation of Audit and Compliance programmes using the Directive for the Protection of Critical Information Infrastructure.
2. Coordinate the development and implementation of Frameworks.
   - Risk Management Framework for designated CIIs and GDIs.
   - Crisis Management Framework for designated CIIs.
   - Audit, Compliance and Monitoring Framework for designated CIIs.
3. Coordinate the development of Sectoral Directives for key CII sectors.
   - Development of Government Sector Directive
   - Development of Energy Sector Directive
   - Development of Health Sector Directive
   - Development of Banking & Finance Sector Directive
   - Development of Information & Communication Technology Sector Directive.
4. Conduct sector scan and analysis to identify potential institutions which qualify as CII for the attention of the Minister for possible designation pursuant to Section 35 of Act 1038.
5. Develop and implement capacity building programmes for designated CII owners.

PHOTO GALLERY


Asaase
Radio100.3
The Voice of Our Land


AFJOC

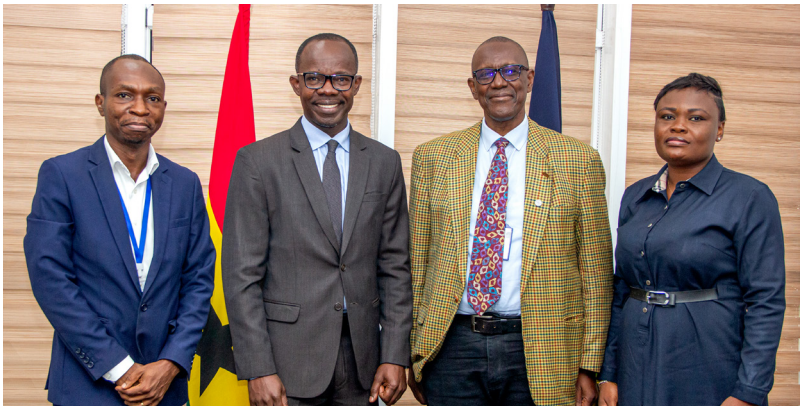

CYBER SECURITY
AUTHORITY
(CSA)


CYBER SECURITY AUTHORITY


Legally Re tered Business according
naian Laws
or Experience of
pers licens


CYBER SECURITY AUTHORITY


CISO Summit




DANTE JEREMY GIKUNDO
ST. PETER'S SENIOR HIGH SCHOOL

CYBER SECURITY AUTHORITY

www.csa.gov.gh

A SAFER DIGITAL GHANA