REPUBLIC
OF GHANA

LEADING AFRICA IN CYBERSECURITY EXCELLENCE

A STRATEGIC ROADMAP

A Secure and Resilient Digital Ghana

www.csa.gov.gh

CYBER SECURITY AUTHORITY
FREEDOM AND JUSTICE
CSA

foreword

The digital transformation of our nation has fundamentally changed how we work, communicate, and live. This new era, however, brings with it a complex landscape of cyber threats that can undermine our progress and compromise our security. To safeguard our digital future, we must remain vigilant and proactive.

Ghana's cybersecurity journey began in 2011 when the then Ministry of Communications, under the leadership of the Former President, H.E. John Evans Atta Mills, with the support of the United Nations (UN) Economic Commission for Africa (UNECA), initiated a process to review Ghana's ICT for Accelerated Development (ICT4AD) policy to include recent developments in ICT and related technical dimensions. Consequently, cybersecurity was identified as one of the four thematic areas to be included in the policy during the review. Following this, an ad-hoc technical committee was constituted to develop a national cybersecurity policy and strategy for Ghana. The work of the committee led to the development and adoption of Ghana's first Cybersecurity Policy and Strategy. This maiden edition served as a cornerstone for strengthening the country's cyber resilience. It focused on securing critical information infrastructure, enhancing cybersecurity governance, and fostering collaborations with both international and local stakeholders. Through capacity building, incident management systems, and regulatory reforms, the strategy aimed to mitigate risks in a rapidly evolving digital environment.

Over the years, Ghana, in collaboration with all stakeholders, has built upon this legacy. The bipartisan work of the seventh Parliament that culminated in the development and passage of the Cybersecurity Act, 2020 (Act 1038) on November 06, 2020, is a landmark piece of legislation that institutionalised our commitment to cybersecurity. This Act laid the groundwork for the establishment of the Cyber Security Authority (CSA), the body mandated to regulate, oversee, and advance the nation's cybersecurity agenda, as well as to address all related matters. The revision of the National Cyber Security Policy and Strategy and the National Child Online Protection Framework, as well as other key achievements spearheaded by the CSA, have led to a significant and progressive rise in Ghana's ranking on the International Telecommunication Union (ITU) Global Cybersecurity Index (GCI). The country is currently ranked as Tier 1 (Role Modelling). This recognition is a testament to our collective resolve and serves as a powerful validation of the strategic decisions we have made.

This three-year cybersecurity strategy is not merely an operational blueprint to guide the CSA in its work; it is a critical component of our broader national vision. In an increasingly digital world, a secure and resilient ecosystem is one of the key foundational pillars on which our 24-Hour Economy Policy, which is to unlock round-the-clock productivity and create new opportunities for our people, rests. Cybersecurity is no longer a peripheral concern; it is a core enabler of our national development agenda.

I call upon all Ghanaians, from public officials and private sector leaders to every citizen, to embrace the implementation of this strategy as a shared responsibility. By working together, we can ensure that our digital transformation achievements and ambitions are not jeopardised and that our nation remains a safe and prosperous place for all.

H.E. John Dramani Mahama
President of the Republic of Ghana

Preface

The digital revolution is no longer a distant prospect; it is our current reality. From the convenience of mobile banking to government e-services, technology has become the driving force behind our national progress. However, this rapid digitalisation introduces a new set of challenges. As we develop a digitally enabled nation, we must remain equally vigilant to ensure its resilience against cyber threats could undermine our efforts. Cybersecurity is more than just a technical matter; it is a crucial element of our national security, economic stability, and public trust.

I am immensely proud of the bipartisan effort that led to the passage of the Cyber Security Act, 2020 (Act 1038). This crucial legislative work was driven by a conviction that our digital ecosystem required a robust legal framework and a dedicated institutional body to govern it. The establishment of the Cyber Security Authority (CSA) marked a key milestone, providing the nation with a central hub tasked with coordinating our defence against cyber threats. A key element of this achievement was the inclusion of the establishment of the Cybersecurity Fund within Act 1038. The objective of this Fund is to provide the essential financial resources to build capacity, support research, and implement a wide range of initiatives that will strengthen our collective cyber resilience.

Our digital transformation ambitions require a coherent, proactive, and sustained effort in cybersecurity development, underpinned by multi-stakeholder involvement. For that matter, this three-year strategy is rooted in the revised National Cyber Security Policy and Strategy that was launched in October 2024. It seamlessly integrates elements of the Government's Reset Agenda, particularly its vision for a 24-hour Economy. We recognise that a thriving, round-the-clock economy, with its increased reliance on digital services and infrastructure, can only be built on a bedrock of strong digital security.

This Strategic document, therefore, serves as the operational blueprint to secure the very foundation of this economic vision, ensuring that our businesses and citizens can innovate, transact, and prosper in a safe and trusted digital environment. It is our social contract to guarantee a secure and resilient digital Ghana, and I call upon all stakeholders to support the CSA in its mandate.

Samuel Nartey George (MP)
Minister for Communication, Digital Technology and Innovations Republic of Ghana

Statement

In an era where the digital landscape is rapidly expanding, in both the public and private sectors, our nation's progress is increasingly reliant on a secure online environment. The revised National Cybersecurity Policy and Strategy (NCPS) serves as the guiding light for Ghana's cybersecurity development, laying the foundational pillars upon which we will develop a secure and resilient digital ecosystem.

With this three-year operational blueprint, we are charting a decisive course. Its purpose is to serve as the roadmap that aligns our immediate priorities with the President of the Republic's overarching vision and the strategic direction of our Sector Minister to secure the foundation of the 24-Hour Economy Policy. We understand that a round-the-clock economy requires round-the-clock security, and this plan provides the structure to achieve just that.

Our success hinges on collaboration. Cybersecurity is a shared responsibility, and this blueprint emphasises the critical role of our multi-stakeholder approach. The CSA's Management under the leadership of its Governing Board, alongside the active partnership of the Joint Cybersecurity Committee and the Industry Forum, will drive these efforts forward. This will ensure that our efforts are inclusive, pragmatic, and responsive to the evolving needs of both the public and the private sector.

As we look to the future, we must continue to innovate and push the boundaries of what is possible. Our efforts are not just for Ghana; they are a beacon for the entire continent. Our ultimate objective is to solidify Ghana's position as a regional and continental leader in cybersecurity excellence.

I call on all of you to join us in this mission to make our vision a reality: "Ghana: **L**eading **A**frica in **C**ybersecurity **E**xcellence" – **L.A.C.E. 2028.**

Divine Selase Agbeti
Ag. Director-General, Cyber Security Authority
Republic of Ghana

1.0. Introduction

The Government of Ghana's Reset Agenda, which seeks to ensure institutional reform, economic stability and social equity, cannot be fully realised without a secure and resilient digital ecosystem.

At its inception in October 2021, the Cyber Security Authority (CSA) set, as its five-year operational vision, the target of Ghana being ranked first in Africa and being counted among the top twenty-five (25) countries in the world in terms of cybersecurity maturity. By September 2024, the outcome of the 5th edition of the ITU GCI indicated that this vision had been largely achieved. Ghana scored 99.27% in the tier-based scoring system adopted for the index. This made the country one of five (5) African countries to achieve Tier 1 (Role Modelling) status and placed it among forty-six (46) countries worldwide to be ranked in this category.

In October 2024, the CSA launched the revised National Cybersecurity Policy & Strategy (NCPS) to direct the national course of cybersecurity development over five (5) years. The Policy Statements and Strategic Imperatives within the NCPS aim to enhance confidence, trust, and security in the country's ICT architecture, and provide clear strategic objectives and initiatives for a secure and resilient digital Ghana.

For the next three (3) years, the vision under the current leadership of the Authority is to consolidate Ghana's position on the continent as a leader in cybersecurity development. This vision has been christened: "Ghana: **L**eading **A**frica in **C**ybersecurity **E**xcellence" – **L.A.C.E. 2028.** This vision is underpinned by a set of strategic initiatives categorised under seven (7) thematic areas, namely, Resilient Foundational Pillars of Cybersecurity; Resilient Digital Ecosystem; Secure Digital Infrastructure; National Capacity Development; Cybercrime Deterrence; Enhanced Cooperation; and Institutional Development. Together, these initiatives form the L.A.C.E. strategic framework (illustrated in Figure 1) and have been picked based on the following criteria:

- Short-term initiatives under the five (5) Strategic Imperatives of the NCPS.
- Cybersecurity-related initiatives from the manifesto of the ruling government.
- Other initiatives that have been prioritised by the Management of the CSA under the leadership of its Governing Board.

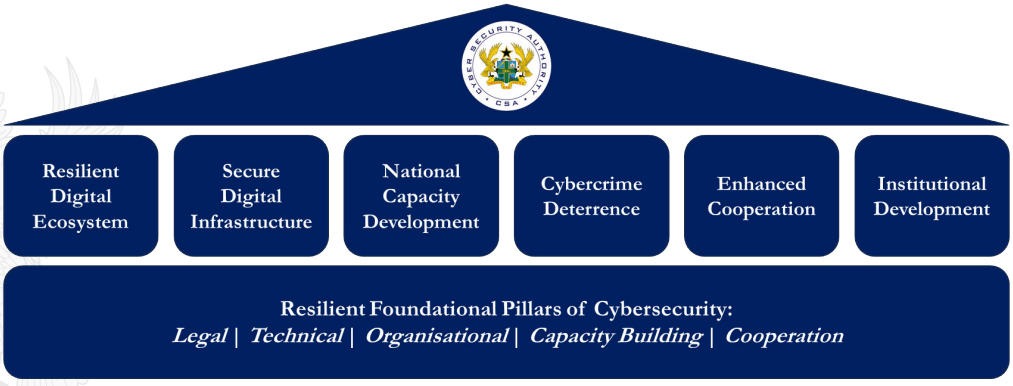

*Figure 1: Conceptual Model for "Ghana: **L**eading **A**frica in **C**ybersecurity **E**xcellence" - **L.A.C.E. 2028***

2.0. Vision, Mission And Core Values Of The Cyber Security Authority

Vision

To ensure a Secure and Resilient Digital Ghana.

Mission

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

Core Values

- Confidentiality
- Inclusiveness
- Integrity
- Commitment
- Reliability
- Professionalism

Mandate Of The Cyber Security Authority (CSA)

- Protection of Critical Information Infrastructure (CIIP)
- Capacity Building & Awareness Creation
- Child Online Protection
- Standards & Enforcement
- Incident Response
- Licensing
- Certification & Accreditation
- Research & Development
- International Cooperation

3.0. Strategic Initiatives

This section details the key initiatives that will contribute to the achievement of the 3-year vision of "Ghana: Leading Africa in Cybersecurity Excellence" – L.A.C.E. 2028.

3.1. Thematic Area 1: Resilient Foundational Pillars of Cybersecurity

The CSA has adopted the pillars outlined in the Global Cybersecurity Index (GCI) as the basis for its Resilient Foundational Pillars of Cybersecurity thematic area. These pillars already underpin the revised National Cybersecurity Policy and Strategy, released in October 2024.

The GCI assesses the commitment of countries to cybersecurity across five pillars, namely:

- Legal: Measuring the laws and regulations on cybercrime and cybersecurity
- Technical: Measuring the implementation of technical capabilities through national and sector-specific agencies
- Organisational: Measuring national strategies and organisations implementing cybersecurity
- Capacity Development: Measuring awareness campaigns, training, education and incentives for cybersecurity capacity development
- Cooperation: Measuring partnerships between agencies, firms and countries

The GCI was launched in 2015 by the International Telecommunication Union to help countries identify areas of improvement and encourage countries to act in building capacity and capabilities under each pillar.

In 2017, Ghana scored 32.6% in the GCI, an indication that many of the key foundational structures for cybersecurity were in their formative stages. In 2020, the country scored 86.69% a testament to the phenomenal work led by the then National Cyber Security Centre, which eventually became the CSA in October 2021. In 2024, Ghana further improved this rating by scoring 99.27% in the 5th edition of the GCI. Notably, the only pillar under which the country was unable to score full marks was Capacity Development.

For the next three (3) years, the target is to maintain or improve the 2024 score by sustaining and/or further improving upon all required metrics under each pillar. Key areas of focus under the Capacity Development pillar are as follows:

S/N	Initiative	Description	Stakeholders
1	Drive Awareness campaigns to reach all target groups	Implement the Safer Digital Ghana Campaign: a multi-platform awareness drive to engage children, the public, businesses and government. Channels to be covered include the print media, radio, TV, social media, information vans, and billboards across the 16 regions of the country.	• CSA • JCC • Media Partners • Relevant MDAs • Non-Governmental Stakeholders
2	Enhance existing capacity-building programmes.	Ensure that persons with specific needs, such as persons with disabilities and the aged, receive attention in cybersecurity capacity building and awareness creation campaigns.	• CSA • JCC • Media Partners • Relevant MDAs • Industry Forum • International Partners
3	Strengthen R&D-related activities in the country	Provide mechanisms for actors in the public and private sectors, as well as academia, to carry out cybersecurity-related R&D activities.	• CSA • JCC • Relevant MDAs • Industry Forum • International Partners
4	Participate in private-public partnerships (PPP) on cybersecurity with foreign companies	Develop and operationalise a framework for private-public partnerships in the cybersecurity sector	• CSA • JCC • Industry Forum • International Partners

Table 1: Resilient Foundational Pillars of Cybersecurity - Initiatives

3.2. Thematic Area 2: Resilient Digital Ecosystem

This thematic area seeks to advance the implementation of initiatives that are crafted to enable Ghana to build a resilient digital ecosystem. This will be facilitated by the sharing of timely and actionable cybersecurity information for proactive detection of threats. It will also encompass the development of the country's human resource capacity for digital risk assessments, advanced cyber security threat detection and incident response.

S/N	Initiative	Description	Stakeholders
1	Operationalise the outstanding five (5) Sectoral Cybersecurity Emergency Response Teams (CERT)	• Operationalise the outstanding five (5) Sectoral CERTs. • Complete integration of all nine (9) Sectoral CERTs into the National CERT.	• CSA • JCC • Relevant MDAs • Industry Forum • International Partners
2	Drive membership of Sectoral and other CERTs into AfricaCERT and the Forum for Incident Response and Security Teams (FIRST)	• Facilitate trust building within cybersecurity teams through the sharing of information and best practices both continentally and globally.	• CSA • Sectoral CERTs • Industry Forum • International Partners
3	Develop and operationalise the National Cybersecurity Contingency Plan	• Implement a comprehensive framework for national cybersecurity incident/ crisis management.	• CSA • JCC • Sectoral CERTs • Relevant MDAs • Industry Forum • International Partners
4	Operationalise the Cyber Risks Early Warning System (EWS)	• Provide situational awareness of cybersecurity threats, especially those concerning CII. • Set up a trusted advisory mechanism on cybersecurity-related matters for both the public and private sectors.	• CSA • JCC • Sectoral CERTs • Industry Forum • International Partners

Table 2: Resilient Digital Ecosystem - Initiatives

Execution of the above initiatives is expected to result in an advanced, inclusive, proactive, interactive, trusted, and responsive incident response architecture.

3.3. Thematic Area 3: Secure Digital Infrastructure

The initiatives under this thematic area are designed to facilitate the deployment of resilient digital infrastructure across the public and private sectors. This comprises Critical Information Infrastructure (CII), Government Digitalisation Initiatives (GDI) or e-Government Services, as well as other digital networks and systems within the private sector.

S/N	Initiative	Description	Stakeholders
1	Establish the National Cybersecurity Risk Management Framework for Critical Information Infrastructure (CII) & Government Digitalisation Initiatives (GDI)	• A framework that will assist in the risk management of all CII Owners and GDIs, as well as the development of risk registers for CII and GDIs.	• CSA • JCC • CII Owners • Relevant MDAs • Industry Forum
2	Establish the Cybersecurity Assurance Programme for CII Sectors and GDI Owners.	• A standards-based framework for CII Owners and GDIs, complemented by regular security auditing and Vulnerability Assessment and Penetration Testing (VAPT).	• CSA • JCC • CII Owners • Relevant MDAs • Industry Forum
3	Establish a National Vulnerability Disclosure Framework.	Robust mechanism to: • Identify and disclose vulnerabilities in the CII Sectors and GDIs • Assess the capabilities of CII and GDI owners to prevent, detect, identify, and recover from cyber attacks	• CSA • JCC • CII Owners • Industry Forum • Relevant MDAs

Table 3: Secure Digital Infrastructure - Initiatives

3.4. Thematic Area 4: National Capacity Development

The initiatives in this thematic area have been selected to birth a formidable cybersecurity research and development ecosystem within the country, enhance cybersecurity awareness, and develop cybersecurity-related education and training programmes that produce qualified and certified cybersecurity professionals. This capacity development will be underpinned by a collaborative public-private framework.

Additionally, the One Million Coders Programme, as well as the establishment of Zonal ICT Parks across the country, are envisaged to be key delivery vehicles for national cybersecurity capacity development.

S/N	Initiative	Description	Stakeholders
1	Operationalise Cybersecurity Certification Scheme	Develop and implement a framework of baseline cybersecurity standards covering both the public and private sectors: • Tiered certification scheme • Auditing framework	• CSA • JCC • National Accreditation Board • Ghana Standards Authority • Other Relevant MDAs • Industry Forum • International Partners
2	Establish a standards framework for cybersecurity products.	• Develop and roll out a framework that sets out baseline standards for cybersecurity software and hardware.	• CSA • JCC • Ghana Standards Authority • Other Relevant MDAs • Industry Forum • International Partners
3	Develop and implement the Child Online Protection (COP) guidelines for educators, parents, industry, children and other stakeholders.	• Operationalise a comprehensive guideline for the industry, ensuring alignment with the Cyber Security Act (2020), Act 1038, the COP Framework, as well as the CSA's Legislative Instrument (secondary legislation).	• CSA • JCC • Ministry of Gender, Children and Social Protection • Ministry of Education • International Partners • Other Relevant MDAs • Industry Forum • International Partners

4	Implement Ghana's National Cybersecurity Organisational Structure	• Identify and align stakeholders on their roles and responsibilities within the structure. • Develop and implement Standard Operating Procedures (SOPs) for national cybersecurity operational coordination.	• CSA • JCC • CII Owners • Industry Forum • Relevant MDAs
5	Integrate cybersecurity education into the curricula at all levels, from basic to tertiary.	• Develop a framework to integrate cybersecurity education into basic, senior secondary education, tertiary and continuing education programmes and courses in Ghana.	• CSA • JCC • Ministry of Education • National Accreditation Board • Other Relevant MDAs • Industry Forum • International Partners
6	Operationalise the 10,000 Cybersecurity Jobs Initiative	Operationalise a three-pronged strategy that adds at least 10,000 jobs to the 24-Hour Economy initiative: • Cybersecurity Workforce Need Assessment • Cybersecurity Workforce Development • Cybersecurity Workforce Deployment	• CSA • JCC • Relevant MDAs • Industry Forum • International Partners
7	Operationalise the Cybersecurity Fund	• Drive stakeholder engagements to activate the various sources of funds to realise the Cybersecurity Fund.	• CSA • JCC • Parliament • Ministry of Finance • Industry Forum • International Partners
8	Implement a policy that allocates at least 30% of government cybersecurity projects and contracts to qualified and licensed local cybersecurity firms.	• Engage stakeholders to define and implement a local-content-oriented policy for the local cybersecurity industry.	• CSA • JCC • Public Procurement Authority • Relevant MDAs • Industry Forum • International Partners

9	Implement the National Cybersecurity Monitoring and Evaluation (M&E) Framework	• Develop evidence-based M&E metrics to measure the impact of strategic initiatives against their objectives. • Deploy a digital platform to document and track the agreed metrics. • Leverage various assessment instruments to collect performance data for the M&E Framework.	• CSA • JCC • Relevant MDAs • Industry Forum
10	Establish a Cyber Innovations Competition	Develop and roll out a framework for a competition that will: • foster innovation • increase awareness of cybersecurity • scout for and develop talent • encourage investments in local cybersecurity startups	• CSA • JCC • Relevant MDAs • Industry Forum • International Partners
11	Develop Ghana's Cybersecurity Research and Development (R&D) framework and roadmap.	Stakeholder engagements to realise a framework and an implementation roadmap that identifies Ghana's cybersecurity research and development needs.	• CSA • JCC • Relevant MDAs • Tertiary Institutions • Industry Forum • International Partners
12	Commission a Cyber Centre of Excellence and the Cybersecurity Research and Development Lab	Stakeholder engagements to realise a Centre dedicated to: • Researching emerging threats • Developing academic programmes, certifications, and workshops • Collecting and analysing cyber threat intelligence, etc.	• CSA • JCC • National Accreditation Board • Relevant MDAs • Industry Forum • International Partners

Table 4: National Capacity Development – Initiatives

The expected outcomes of the initiatives outlined above are to:

- Foster self-reliance in cybersecurity research and development.
- Establish the country's status as a Cybersecurity Hub within the ECOWAS sub-region and on the continent.
- Raise highly cyber-aware citizens (Children, the Public, Businesses, and Government).

3.5. Thematic Area 5: Cybercrime Deterrence

The revised NCPS advocates a deterrence approach to cybercrime. For that matter, the initiatives selected under these thematic areas are designed to ensure that cybercrime becomes a high-risk venture for potential perpetrators while enhancing the security posture of Ghana's digital infrastructure.

By 2028, the expectations are the following:

- Measurable reduction in the impact of cybercrime on the Ghanaian economy
- Institution of offensive and defensive cyber capabilities
- Adequately equipped law enforcement and criminal justice authorities that enforce existing and future cybercrime legislation

S/N	Initiative	Description	Stakeholders
1	Establish a specialised court for prosecuting cybercrime cases.	• Conduct stakeholder workshops to develop Ghana's Cyber Court Framework. • Train target stakeholder groups in cyber law, digital evidence handling. • Conduct training sessions on the developed framework for selected judges, prosecutors, law enforcement officers, investigators and other judicial support staff.	• CSA • JCC • Office of the Attorney-General and Ministry of Justice • Judicial Service • National Security Council Secretariat • Ghana Bar Association
2	Run an annual training programme for Judges, Prosecutors and Investigators	• Leverage status as a GLACY-E+ hub country to run continuous training for Judges, Prosecutors and Investigators through the integration of cybercrime and digital evidence courses into the curriculum of criminal justice sector training institutions	• CSA • JCC • International Partners • Ghana Bar Association • Judicial Training Institute

3	Establish the National Digital Forensics Laboratory.	• Develop standard operating procedures and relevant guidelines to support cybercrime and cybersecurity investigations and digital forensics case management for law enforcement agencies.	• CSA • JCC • National Security Council Secretariat
4	Institute an annual training programme on cybercrime and digital evidence for members of the Ghana Bar Association.	• Collaborate with relevant stakeholders to create a continuous training programme on cybercrime and digital evidence for members of the Ghana Bar Association.	• CSA • JCC • International Partners • Ghana Bar Association • Judicial Training Institute
5	Establish at least 5 Regional Cybercrime Units covering the main zones of the country.	• Set up cybercrime units to support cybercrime response in identified “hotspots” to receive complaints and provide the first response on cybercrime cases.	• CSA • JCC • Ghana Police/CID • National Security Council Secretariat • International Partners

Table 5: Cybercrime Deterrence - Initiatives

3.6. Thematic Area 6: Enhanced Cooperation

The unprecedented level of borderless interconnectedness that digitalisation brings calls for the focused cultivation of partnerships, cooperation frameworks and information sharing networks at the national, regional and global levels. Hence, the achievement of the initiatives identified under these thematic areas is expected to result in:

- Enhanced influence in the West-African community and beyond
- A free, open, innovative, and secure cyberspace
- Strengthened formal and informal cooperation mechanisms with all relevant stakeholders

S/N	Initiative	Description	Stakeholders
1	Operationalise the Cybersecurity Industry Forum	• Facilitate the finalisation and adoption of the Industry Forum's constitution and Industry Code through the work of the interim Facilitation Committee. • Oversee transition from Facilitation Committee to leadership team led by Facilitator (Section 81(6).	• CSA • Industry Players
2	Sign the UN Convention on Cybercrime & Participate in Open-Ended Working Group (OEWG) Processes	• Complete all required stakeholder engagements and briefs. • Support completion of the ratification process.	• CSA • JCC • Ministry of Foreign Affairs • Office of the Attorney-General and Ministry of Justice • National Security Council Secretariat • Industry Forum • International Partners
3	Facilitate the Operationalisation of ANCA's 5-year Vision and Strategy	• Drive implementation of ANCA's goals that fall within the stipulated time as Chair of ANCA, including organising a continental cybersecurity conference to build awareness of ANCA and its objectives.	• CSA • Members of ANCA
4	Join the International Countering Ransomware Initiative (CRI)	• Complete process to join the initiative whose goal is to collectively build resilience against ransomware, disrupt the criminal ecosystem, and develop international policy	• CSA • JCC • Ministry of Foreign Affairs • Industry Forum • International Partners

5	Participate in the World Summit on the Information Society (WSIS)+20 Review Process	• A comprehensive multistakeholder effort, culminating in a high-level meeting in 2025 to assess twenty (20) years of WSIS outcomes and shape a forward-looking, inclusive, and development-oriented vision for the global information society	• CSA • International Stakeholders
6	Coordinate the Joint Cybersecurity Committee to develop a Digital Fraud Monitoring System.	• Leverage the leadership of the JCC to develop a Digital Fraud Monitoring System to detect, prevent, and respond to fraudulent activities that occur across digital platforms.	• CSA • JCC • Industry Forum
7	Ratify the Second Additional Protocol of the Budapest Convention.	• Conduct stakeholder engagements and awareness creation sessions leading to the adoption of the new mechanisms and provisions included in the Budapest Convention.	• CSA • JCC • Ministry of Foreign Affairs • Office of the Attorney-General and Ministry of Justice • National Security Council Secretariat • Industry Forum • International Partners
8	Operationalise the Pall Mall Process Code of Practice	The Code of Practice is a non-binding framework for nations to tackle the proliferation and irresponsible use of commercial cyber intrusion capabilities. This initiative will: • Engage national stakeholders to develop an adoption framework and roadmap. • Support advocacy efforts designed to engage other African countries to adopt the code.	• CSA • JCC • Ministry of Foreign Affairs • Office of the Attorney-General and Ministry of Justice • National Security Council Secretariat • Industry Forum • International Partners

Table 6: Enhanced Cooperation - Initiatives

3.7. Thematic Area 7: Institutional Development

The CSA, as a creation of the Cybersecurity Act, 2020 (Act 1038), needs to be fully empowered, equipped and funded to consistently deliver on its mandate. Thus, the institution needs to be carefully nurtured, leveraging the following initiatives to ensure the vision of a secure and resilient digital Ghana is achieved. The following table captures the initiatives planned under this thematic area:

S/N	Initiative	Description	Stakeholders
1	Review and amend the Cybersecurity Act, 2020 (Act 1038)	• Coordinate with the Ministry of Communication, Digital Technology and Innovations (MOCDTI), along with relevant stakeholders, to position the Cybersecurity Act to respond to current and unpredictable challenges posed by the ongoing adoption of digital technology.	• CSA • JCC • Parliament • Office of the Attorney-General and Ministry of Justice • Industry Forum • International Partners
2	Operationalise Legislative Instruments	• Coordinate with MOCDTI to complete the process to activate the Legislative Instruments of the Authority.	• CSA • JCC • Parliament • Office of the Attorney-General and Ministry of Justice
3	Establish a dedicated regulatory enforcement division, i.e. CSA Regulatory Enforcement Team (CRET).	• Set up and empower a dedicated team to conduct regulatory compliance assessments and enforcement actions to enhance the resilience of Ghana's digital ecosystem.	• CSA • JCC • Office of the Attorney-General and Ministry of Justice • National Security Council Secretariat • Industry Forum • International Partners
4	Establish Regional Offices	Regional hubs to host teams for: • Outreach work, e.g. awareness creation in educational institutions, town-hall sessions, local radio/TV engagements • Interface to the National CERT PoC • Interface with local law enforcement agencies. • On-the-ground surveillance and informant coordination.	• CSA • JCC • Relevant MDAs • National Security Council Secretariat

5	Implement ISO 27001 certification programme	• Formally certify the information security management system of the Authority.	• CSA • JCC
6	Develop an updated National Cybersecurity Policy and Strategy	• Compile the third edition of Ghana's National Cybersecurity Policy and Strategy, considering developments at the national, continental and global level.	• CSA • JCC • Relevant MDAs • Industry Forum • International Partners

Table 7: Institutional Development – Initiatives

4.0. Monitoring And Evaluation

The Monitoring and Evaluation mechanisms, as outlined in the revised National Cybersecurity Policy and Strategy, 2024, will be leveraged to measure the outcomes of the various initiatives in this 3-year strategy document.

5.0. Conclusion

The strategic initiatives outlined in this document are designed to address priority cybersecurity objectives within the next three years. Granted that the required resources are allocated, the delivery of these initiatives is expected to be completed by 2028. It is crucial to emphasise that the operationalisation of the Cybersecurity Fund, as mandated in Section 29 of the Cybersecurity Act, 2020 (Act 1038), is a prerequisite to achieve the vision captured in this 3-year plan and, by extension, the broader National Cybersecurity Policy and Strategy.

6.0. ANNEX - Glossary of Terms

Cyberattack - A deliberate attempt to damage, disrupt, or gain unauthorised access to a computer, computer system or electronic communication network.

Cybercrime - includes both cyber-dependent and cyber-enabled crimes:

- **Cyber-dependent crimes** - Crimes committed using ICT devices, and where the devices are both the tool for committing the crime, and the target of the crime.
- **Cyber-enabled crimes** - Traditional crimes which can be increased in scale or reach using computers, computer networks or other ICTs.

Cybersecurity - The state in which a computer or computer system is protected from unauthorised access or attack for the purpose of ensuring that

a. the computer or computer system continues to be available and operational;

b. the integrity of the computer or computer system is maintained; and

c. the integrity and confidentiality of information stored in, processed by or transmitted through the computer or computer system is maintained.

Cyberspace - The interdependent network of information technology infrastructure that includes the internet, telecommunications networks, computer systems, internet-connected devices and embedded processors and controllers.

Identity Theft - The deliberate use of someone else's identity, usually as a method to gain access, financial advantage, or other benefits in the other person's name.

Industry Forum - a body designated to work with the CSA to develop Ghana's cybersecurity ecosystem within a collaborative regulatory framework. It includes the Private Sector, Academia & Research Institutions, Civil Society, as well as Professional and Industry Associations.

Malware - Any software intentionally designed to cause damage to a computer, server, client, or computer network.

MDAs - Consists of Government Ministries, Departments and Agencies.

National CERT - A Computer Emergency Response Team responsible for facilitating and coordinating incident response procedures at the national level.

Ransomware - Malicious software that denies the user access to their files, computer or device and in some cases threatens to publish the user's private data unless a ransom is paid.

Risk - The potential that a threat will exploit a vulnerability of an information system and cause harm.

REPUBLIC
OF GHANA