



REPUBLIC  
OF GHANA



# DIRECTIVE FOR THE PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE (CII)



*A Secure and Resilient Digital Ghana*



Copyright ©2021 Cyber Security Authority, Ghana. All rights reserved.  
Published by the Cyber Security Authority (CSA)

# DIRECTIVE FOR THE PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE (CII)

## REPUBLIC OF GHANA

(Pursuant to Sections 35 to 40 and 92  
of the Cybersecurity Act, 2020 (Act 1038))





# Table of Content

Foreword	<b>2</b>
Preface	<b>4</b>
1. Background	<b>6</b>
2. Objective	<b>7</b>
3. Applicability	<b>7</b>
4. Designated CII Sectors	<b>7</b>
5. Baseline Cybersecurity Requirements for CII	<b>9</b>
6. The Mandate of the Cyber Security Authority (CSA)	<b>12</b>
7. Audit and Compliance	<b>13</b>
8. Request for Clearance and Guidance	<b>14</b>
9. Sanctions	<b>15</b>
10. Entry into Force	<b>15</b>
Acronyms	<b>16</b>
Definitions	<b>16</b>



## Foreword



The Ministry of Communications and Digitalisation is committed to ensure that the digital interventions rolled out over the past few years as part of the *Digital Ghana Agenda* are secured from the prevailing cyber-attacks. As a cybersecurity enabler, the government has demonstrated its commitment by way of implementing priority initiatives to support Ghana's cybersecurity development. The enactment of the Cybersecurity Act, 2020 (Act 1038) is one of such enabling interventions for Ghana's cybersecurity development.

With cyber-attacks against critical information infrastructures (CIIs) on the ascendency, Act 1038 provides the legal basis (specifically Sections 35 to 40) for the implementation of relevant measures for the protection of Ghana's CIIs. In accordance with Section 35 of the Act, 13 sectors have been designated as Ghana's CII sectors namely, *National Security and Intelligence, Information and Communications Technology (ICT), Banking and Finance, Energy, Water, Transportation, Health, Emergency Services, Government, Food and Agriculture, Manufacturing, Mining and Education*. Across the 13 sectors, a number of institutions in the public and private sectors have been notified of their designation as Critical Information Infrastructure Owners.

The *Directive for the Protection of Critical Information Infrastructure* is the first among a number of interventions to be introduced as part of the implementation of Act 1038. The Directive establishes baseline cybersecurity requirements for all designated CII Owners. The Directive further aligns with the five strategic imperatives of our National Cybersecurity Policy and Strategy, namely *Build a Resilient Digital Ecosystem, Secure Digital Infrastructure, Develop National Capacity, Deter Cybercrime and to Strengthen Cooperation*. Ghana remains one of the few countries on the African continent to have formalised a national level regulation for the protection of critical information infrastructures and this has been done to safeguard our investments in our digitalisation programmes. We acknowledge that Ghana's digital ecosystem cannot be fully insulated from cyber-attacks but these strides undoubtedly position our country with respect to our readiness to mitigate potential cyber-attacks.

As a policy direction and in accordance with Act 1038, the Cyber Security Authority (CSA), shall publish relevant Guidelines for the continuous identification, registration and cyber risk





management of all Ghana's CIIs. A cyber resilient CII ecosystem itself is an enabler for digital innovations, trust and confidence building in the use of digital services with a huge potential to contribute to the growth of our GDP by improving revenue generation and economic development, among others.

In this regard, the government will continue to prioritise the development of the cybersecurity sub-sector of our digital ecosystem. Protection of CIIs is therefore a prime undertaking to ensure a sustained digital transformation. I, therefore, entreat all stakeholders to fully comply with this Directive for a **Secure and Resilient Digital Ghana**.

**Mrs Ursula Owusu-Ekuful (MP)**

*Minister for Communications and Digitalisation*

*Republic of Ghana*



## Preface

The introduction of the Cybersecurity Act, 2020 (Act 1038) establishes the Cyber Security Authority (CSA). Section 3 of Act 1038 mandates the Authority to regulate cybersecurity activities and to promote the development of cybersecurity in the country. One critical mandate of the Authority, according to Section 3(c), is to regulate owners of critical information infrastructure in respect of cybersecurity activities to ensure a secured and a resilient digital ecosystem.

The designation of critical information infrastructures (CIIs) by the Minister responsible for cybersecurity matters pursuant to Section 35 of Act 1038 is timely in view of the escalating cyber-attacks targeting the various CII sectors around the world, Ghana inclusive. According to the World Economic Forum's Global Risks Report 2020, cyberattacks against CIIs are rated as the fifth (5th) top risk in 2020, and cybercrime damages have been estimated to reach US\$6 trillion - which would be equivalent to the GDP of the world's third-largest economy. Ghana, like many other countries has suffered from different forms of cyber-attacks including specific attacks on the government, financial, energy, health, and the education sectors among others. The action by the Minister, pursuant to Section 35 of Act 1038, therefore provides a clear regulatory and operational direction for the protection of all designated CIIs.

The Directive provides the baseline information and cybersecurity requirements for all designated CIIs, irrespective of the maturity level of the CII Sector or the CII institution. The Directive further outlines technical and organisational measures to be adopted by designated CII owners in protecting the CII systems and networks. Based on the provisions in Act 1038, the Authority shall continue to monitor the developments in the digital ecosystem and will provide timely advice to the sector Minister for designation of any identified CII.

In exercising its regulatory functions provided in Act 1038, the Authority will engage with all designated CII Owners and industry stakeholders to implement the required cybersecurity best practices to achieve a robust cybersecurity for Ghana's CII sectors.





The Cyber Security Authority is looking forward to engage with all designated CII Owners and relevant sectoral stakeholders for the full implementation of the Directive for a **Secure and Resilient Digital Ghana**.

**Dr Albert Antwi-Boasiako**

*Ag. Director-General*

*Cyber Security Authority (CSA)*



Critical Information Infrastructure (CII) constitutes assets (real/virtual), networks, systems, processes, information, and functions that are vital to the nation such that their incapacity or destruction would have a devastating impact on national security, the economy, public health and/or safety. CII may comprise a number of different infrastructures with essential interdependencies and critical information flows between them. The Cybersecurity Act, 2020 (Act 1038) defines a critical information infrastructure as a *computer system* or computer network that is essential for national security or the economic and social well-being of citizens.

Cyber-attacks against CIIs are increasing, the magnitude, frequency and impact of such security incidents can impede the pursuit of economic activities, generate substantial disruption to critical services, financial losses, undermine public confidence, and cause major disruption to our economy. Recent attacks on the power grids, electoral systems, payment systems and healthcare systems around the world bring to bear the imminent threats to Ghana's CII. It's only a matter of time before we also fall victim, and we must be prepared for this eventuality.

In the last few years, Ghana has implemented a number of digitalisation initiatives as we modernise networks and information systems to meet relevant developmental agenda, both in the public and the private sectors, and to facilitate the growth of the economy. Some of these networks and information systems form a substantial part of Ghana's CII. They underpin many of the critical services used in daily life, from functions as diverse as financial payments to air traffic control.

The protection of CII is the shared responsibility of both public and private organisations that own and operate CIIs. To ensure a safer and resilient digital ecosystem, there is a need to adopt a framework to ensure the confidentiality, integrity, and availability of Ghana's CII and to minimise the likelihood and impact of successful cyber-attacks against our CII. Ghana must secure its infrastructure, deter cybercrime, develop national capacity, build a resilient digital ecosystem relative to cybersecurity, and strengthen cybersecurity cooperation among critical sectors. The protection of CII constitutes the backbone of Ghana's digital resiliency.



## Objective

The objective of this Directive is to operationalise the provisions of Sections 35 to 40 and Section 92 of the Cybersecurity Act, 2020 (Act 1038):

- 1 | According to Section 92(1) of the Cybersecurity Act, 2020, the Authority may issue directives to an owner of a critical information infrastructure, a cybersecurity service provider, or a service provider for the purpose of ensuring the cybersecurity of the country.
- 2 | This Directive;
- a) Establishes the baseline cybersecurity requirements for all *designated CII Owners* pursuant to Act 1038;
  - b) Establishes the requirements and procedures for incident response including reporting mechanisms of cybersecurity incidents by *designated CII Owners*;
  - c) Establishes the procedures for audit and compliance pursuant to Section 38 of the Cybersecurity Act, 2020 (Act 1038).

## Applicability

This Directive shall apply to all *designated CII Owners*, an individual or entity authorised by the Owner of the CII.

## Designated CII Sectors

The following are the designated CII sectors for Ghana as per Gazette Notice No. **132**, consistent with Section 35 of the Cybersecurity Act:

- |  |                        |
|--|------------------------|
| → National Security and Intelligence       | → Health               |
| → Information and Communication Technology | → Emergency Services   |
| → Banking and Finance                      | → Government           |
| → Energy                                   | → Food and Agriculture |
| → Water                                    | → Manufacturing        |
| → Transport                                | → Mining               |
|  | → Education            |



All *designated CII Owners* shall adhere to the following baseline security requirements to ensure the protection of CIIs.

### 5.1 Policy

A *designated CII Owner* shall adopt the following Policy measures for the protection of the designated CII:

- a) A *designated CII* is required to develop and implement a *Cybersecurity Policy* which adequately addresses CII risks, consistent with international best practices relevant to the identified sector.
- b) A *designated CII Owner* is required to implement and comply with a specific policy directive issued or approved by the CSA.
- c) A designated CII Owner shall appoint an accountable officer of a senior management level rank and require that he/she assumes a proactive approach to Cybersecurity Governance, Policy and Strategy of the *designated CII Owner*.
- d) The *Cybersecurity Policy* adopted should be approved by the Board or Directors of the *designated CII Owner*.



- e) The approved *Cybersecurity Policy* shall be reviewed at least once a year, consistent with identified risks and threats affecting the specific CII sector.
- f) The Cybersecurity Policy should address data protection concerns of the *designated CII Owner*, consistent with the Data Protection Act, 2012 (Act 843).



A *designated CII Owner* shall adopt the following *Technical and Organisational Measures* for the protection of the designated CII. A *designated CII Owner* shall:

- a) Identify, classify and catalogue all CII assets.
- b) Control and manage access to CII systems and services.
- c) Implement relevant security measures to mitigate cyber risk posed by employees, customers, suppliers, service providers, and other third-party affiliates.
- d) Conduct security screening on all personnel who handle CII information or data in the *designated CII*.
- e) Conduct appropriate level of information and cybersecurity awareness and training for all employees of the *designated CII Owner*.



- f) Implement appropriate security monitoring and response process for timely detection of cybersecurity incidents targeting the designated CII.
- g) Implement relevant physical security measures for the physical protection of CII systems and its associated dependent assets and systems.
- h) Implement relevant infrastructure and cybersecurity measures to mitigate equipment failure including maintenance and software updates.
- i) Develop, regularly test and update business continuity and disaster recovery plan to ensure adequacy of such plans to support incident response and security redundancy operations.
- j) Conduct a quarterly cybersecurity risk assessment to identify existing vulnerabilities to which the *designated CII* is exposed.
- k) Conduct yearly cybersecurity audits in compliance with this Directive and the Cybersecurity Act, 2020 (Act 1038).
- l) Create and keep a cybersecurity risk register which catalogues and profiles the various information and cyber risks targeting the *designated CII*.
- m) Conduct and participate in cybersecurity activities in collaboration with the CSA and other CII sectors for the purposes of testing the state of readiness of designated CII Owners in responding to cybersecurity incidents.
- n) Adopt relevant international cybersecurity best practices, frameworks, and standards approved by the CSA.
- o) Ensure that source codes of critical systems are kept in escrow





### 5.3 Incident Reporting

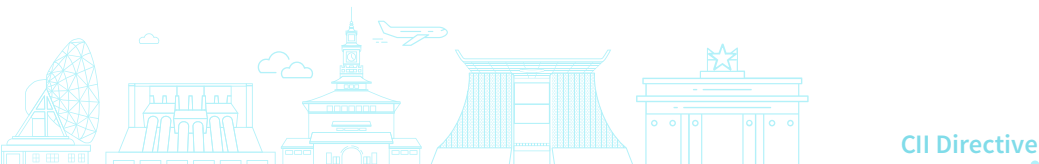
A *designated CII Owner* shall:

- a) In the event of a cybersecurity incident, investigate, report and mitigate impact of the incident according to the cybersecurity standards required by the CSA.
- b) Report all *cybersecurity incidents* to relevant Sectoral CERTs or in case of its non-existence, directly to the National Computer Emergency Response Team (CERT-GH) of the CSA within twenty-four (24) hours of becoming aware of an incident pursuant to Section 39 (1) of Act 1038.
- c) Establish a Point of Contact for reporting cybersecurity incidents and receiving cybersecurity information, including security advisories relevant to the particular *designated CII* sector.
- d) Disclose and report any *vulnerabilities* identified or discovered through internal or external security audits and assessments, within 72 hours of identifying or discovering the vulnerability.

## The Mandate of the Cyber Security Authority (CSA)

6

- a) The CSA shall provide support and guidance to a *designated CII* either through *Sectoral CERTs* or directly to the *designated CII Owner* pursuant to the implementation of this Directive and the Cybersecurity Act, 2020.



- b) The CSA has the overall oversight responsibility to ensure the implementation of the Directive, through collaboration with the Sectoral CERTs, international institutions, or directly with the *designated CII Owners*.
- c) The CSA shall be responsible for coordinating with relevant *Sectoral CERTs* to produce coherent directives, reports, and engagement with *designated CII Owners*.

## Audit and Compliance

7



A *designated CII Owner* shall comply with the following Audit measures for the protection of the designated CII:

- a) The CSA shall conduct an audit of a *designated CII* to ensure compliance with this Directive in adherence to Section 38(2) of the Cybersecurity Act, 2020 (Act 1038).
- b) A *designated CII* shall submit copies of reports covering audits, risk register and any cybersecurity activities conducted, as required in this Directive.
- c) An audit may be carried out by the CSA or its authorised auditor to establish or confirm an audit activity already conducted by the *designated CII Owner*.
- d) A designated CII shall communicate any planned significant change to a designated CII



including changes made to the design, configuration, security, or operation of the CII that will have an impact on the availability of service to the CSA before final board approval.

- e) A designated CII shall seek clearance from the CSA within one (1) month prior to any *major organisational change* in operation, personnel, and infrastructure. Failure to comply with this Directive shall be subject to applicable sanctions in Section 36(4) of the Cybersecurity Act, 2020.
- f) The CSA may issue any additional directive to a *designated CII Owner* without any notice and a *designated CII Owner* shall comply.
- g) A *designated CII Owner* who fails to comply with this Directive shall be subject to applicable sanctions specified in the Second Schedule of the Cybersecurity Act, 2020.

## Request for Clearance and Guidance

8



Any person or entity that seeks to undertake a lawful activity which could impact on the confidentiality, integrity and availability of critical information infrastructure or its associated dependent assets and systems shall make a written request for clearance and guidance from *the Minister* responsible for cybersecurity matters through the CSA.





A person who fails to comply with this Directive shall be subject to applicable criminal and administrative sanctions as provided in Section 92(2) of the Cybersecurity Act, 2020 and other relevant enactments.

## Entry into Force

10

This Directive shall come into effect on **October 1, 2021**.



# Acronyms

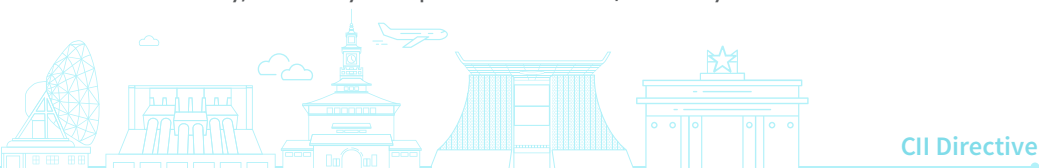
For the purpose of this Directive:

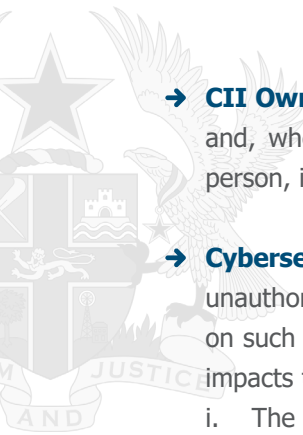
- a) **CII** – Critical Information Infrastructure
- b) **CSA** – Cyber Security Authority
- c) **CERT** – Computer Emergency Response Team

## Definitions

For the purpose of this Directive:

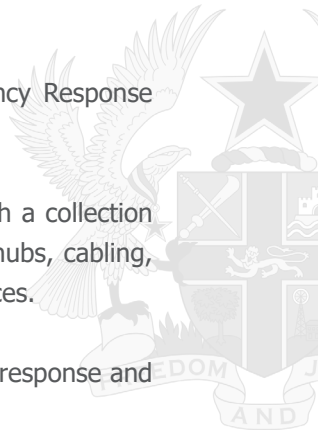
- **Authority** means the Cyber Security Authority (CSA) established under Section 2 of the Cybersecurity Act 2020.
- **Computer** means an electronic, magnetic, optical, electrochemical, or other data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
- **Computer Emergency Response Team** includes a group of experts who are tasked with operations supporting the detection, analysis, and containment of a cyber incident and the response and involves qualified personnel, technology systems, and processes to handle incident response operations.
- **Computer System** means an arrangement of interconnected computers that is designed to perform one or more specific functions, and includes
  - (i) an information system; and
  - (ii) an operational technology system, a programmable logic controller, a supervisory control and data acquisition system, or a distributed control system
- **Critical Information Infrastructure** means a computer or computer system designated under subsection (1) of section 35 of the Cybersecurity Act 2020. They refer to assets (real/virtual), networks, systems and functions that are so vital to the nation such that their incapacity or destruction would have a devastating impact on national security, economy and public health and/or safety.





- **CII Owner** means the legal owner or operator of the critical information infrastructure and, where the critical information infrastructure is jointly owned by more than one person, includes every joint owner.
- **Cybersecurity Incident** means any act or attempt, successful and unsuccessful, to gain unauthorised access to, disrupt or misuse an information system or information stored on such information system. This refers to a disruptive effect on a CII that significantly impacts the following cross-sectorial factors:
  - i. The number of users relying on that service
  - ii. The dependency of other sectors CII sectors on the service provided by that entity;
  - iii. The impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety;
  - iv. The market share of that entity;
  - v. The geographic spread regarding the area that could be affected by an incident; and
  - vi. The importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.
- **Cybersecurity Policy** is a formal set of rules by which CII owners must abide by. Its purpose is to inform CII owners of their obligatory requirements for protecting the technology and information assets of the critical sector.
- **Designated CII** means a computer or computer system designated under subsection (1) of section 35 of the Cybersecurity Act 2020.
- **Designated CII Owner** means the legal owner or operator of a designated critical information infrastructure. This refers to entities responsible for investments in, and/or day-to-day operation of, a particular asset, system, or part thereof designated as a CII under this Directive.
- **Major Organisational Change** refers to any operational or organisational change that impacts critical business service delivery or presents an adverse risk to the business service such as transfer of ownership of all or part of the business service.





- **National CERT (CERT-GH)** is the Ghana National Computer Emergency Response Team established under Section 41 of Act 1038.
- **Networks** refers to an open communications medium implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, base stations, and technical control devices.
- **Point of Contact** means the 24/7 contact point established for incident response and coordination with CII owners.
- **Protection** means all activities aimed at ensuring the functionality, confidentiality, integrity and availability, of critical information infrastructure in order to deter, mitigate and neutralise a threat, risk, or vulnerability.
- **Regulators** refers to an organisation responsible for supervising a regulated sector.
- **Sectoral Computer Emergency Response Team** means teams that have been established by the Authority to operate in a specific sector or institution pursuant to Section 44 of the Cybersecurity Act, 2020.
- **Security screening** – Security checks conducted by the Cyber Security Authority or an authorised National Security institution on staff and those operating CII.
- **Technical and Organisational Measures** are the functions, processes, controls, systems, procedures and measures taken to protect and secure the information assets that an organisation processes.
- **Vulnerability** refers to a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.





# Designated CII Sectors

National Security  
& Intelligence

Information &  
Communication  
Technology (ICT)

Banking and Finance

Energy

Water

Transport

Health

Emergency Services  
NATIONAL  
AMBULANCE  
SERVICE

Government

Food and Agriculture

Manufacturing

Mining

Education



*A Secure and Resilient Digital Ghana*