



For Immediate Release

CYBER SECURITY AUTHORITY BEGINS THE IMPLEMENTATION OF LICENSING AND ACCREDITATION TODAY, MARCH 1, 2023

The Cyber Security Authority (CSA) today commences the implementation of licensing Cybersecurity Service Providers (CSPs), accrediting Cybersecurity Establishments (CEs) and Cybersecurity Professionals (CPs), pursuant to the Cybersecurity Act, 2020 (Act 1038), sections 4(k), 49, 50, 51, 57 and 59.

The purpose of the regime is to ensure regulatory compliance with the Cybersecurity Act, 2020 (Act 1038) and to certify that CSPs, CEs and CPs offer their services in accordance with approved standards and procedures in line with domestic requirements and industry best practices.

Scope of Licence and Accreditation

Given the critical role Cybersecurity Establishments such as digital forensic laboratories and managed cybersecurity services play in securing Ghana's digital ecosystem, it is imperative that processes and technology used by such establishments are in line with international best practices and standards adopted by the Authority. It has therefore become essential that the Authority, in line with Section 59(3) of Act 1038, takes the necessary measures such as licensing CSPs and accrediting CEs and CPs to ensure that recognised standards have been met.

The regulatory process starts with the licensing of existing and new CSPs, which will subsequently be followed by the accreditation of CEs and CPs.

CSA will license CSPs and accredit CPs with requisite expertise in **Vulnerability Assessment and Penetration Testing, Digital Forensics Services, Managed Cybersecurity Services, Cybersecurity Governance, Risk and Compliance.**

Accreditation to Cybersecurity Establishments will consider **Digital Forensics Facility and Managed Cybersecurity Service Facility.**

Under the regime, existing CSPs, who are already engaged in the business of providing cybersecurity services will be given six months (from March 1 to September 30, 2023) to apply for a licence. A CSP who fails to obtain a licence within this period will have to cease operation until a licence is obtained from the Authority.



Benefits to industry and the country

- It has become necessary that the industry is regulated to control cybersecurity risks and protect the interests and safety of the Public, Children, Businesses, and Government. With the increasing rate of cybercrimes, CSPs, CEs and CPs have become critical components for mitigating cybersecurity threats and vulnerabilities within Ghana's fast-developing digital ecosystem in line with the Cybersecurity Act, 2020 (Act 1038).
- Cybersecurity services by the nature of their operations are intrusive, and as a result, CSPs, CEs and CPs always gain access to clients' critical information assets, thereby gaining knowledge of existing vulnerabilities and sensitive information, which could be potentially abused or exploited. It is also possible to have CSPs, CEs, and CPs who may not be competent or who may employ substandard processes in their offerings to the detriment of Ghana's digital ecosystem. In addition, some businesses or government agencies lack the capability of ascertaining the credibility or qualification of CSPs, CEs or CPs especially, since there is no repository of licensed and accredited CSPs, CEs or CPs. This process is to ensure that the targeted entities have the requisite skillset and competence and meet the established standards for offering sufficient protection of the computer systems and networks in the country's digital ecosystem.
- The regulatory exercise will provide greater assurance of cybersecurity and safety to consumers, and to raise the quality of Cybersecurity Service Providers' deliveries, thereby improving and maintaining standards that offer baseline protection to Ghana's digital ecosystem.
- It will ensure that qualified professionals with the appropriate certification, provide cybersecurity services to support a secure and resilient digital ecosystem, and consequently give recognition to the cybersecurity profession as a critical profession to support and sustain the current digital transformation agenda.
- Furthermore, national security considerations are driving regulations in the sector to ensure only qualified persons and institutions in good standing undertake these critical services. The Government, through the CSA, regulates the sector by providing a licensing framework in accordance with Sections 49 to 59 of Act 1038 to guarantee that CSPs, CEs and CPs attain a higher level of



compliance with Act 1038 and standards in line with international best practices. This is to provide assurance to the public and other key stakeholders that the cybersecurity services they procure from the industry are effective in securing their assets and processes.

- Section 57 of Act 1038 mandates the CSA to establish a mechanism to accredit cybersecurity professionals. Such an accreditation process provides recognition to accredited cybersecurity professionals, who have proven demonstrable competence in their cybersecurity domain. Section 59 of Act 1038 further mandates the CSA to enforce cybersecurity standards and monitor compliance by the public and private sectors including Cybersecurity Establishments or institutions.

Consequences of non-compliance

Cybersecurity Service Providers (CSPs) who engage in the business of providing cybersecurity services without the requisite licence after September 30, 2023, shall be in contravention of the Cybersecurity Act, 2020 (Act 1038) and shall be liable to pay administrative penalties. However, a CSP who applies for a licence by September 30, may continue to provide its service until a decision on the application has been made by the Cyber Security Authority. A licence or accreditation granted is valid for two (2) years from the date of issuance as provided for in Section 53(1) of Act 1038.

Further information on the licensing and accreditation process is available at www.csa.gov.gh.

Queries on the process may be sent to compliance@csa.gov.gh.

Issued by
Cyber Security Authority
Accra, March 1, 2023