WEST VIRGINIA CODE: §5a-6B-2

§5A-6B-2. Definitions.

As used in this article:

"Cybersecurity framework" means computer technology security guidance for organizations to assess and improve their ability to prevent, detect, and respond to cyber incidents.

"Cyber incident" means any event that threatens the security, confidentiality, integrity, or availability of information assets, information systems, or the networks that deliver the information.

"Cyber risk assessment" means the process of identifying, analyzing and evaluating risk and applying the appropriate security controls relevant to the information custodians.

"Cyber risk management service" means technologies, practices and policies that address threats and vulnerabilities in networks, computers, programs and data, flowing from or enabled by connection to digital infrastructure, information systems or industrial control systems, including, but not limited to, information security, supply chain assurance, information assistance and hardware or software assurance.

"Enterprise" means the collective departments, agencies and boards within state government that provide services to citizens and other state entities.

"Information custodian" means a department, agency or person that has the actual custody of, or is responsible for the accountability for a set of data assets.

"Plan of action and milestones" means a remedial plan, or the process of accepting or resolving risk, which helps the information custodian to identify and assess information system security and privacy weaknesses, set priorities and monitor progress toward mitigating the weaknesses.

"Privacy impact assessment" means a procedure or tool for identifying and assessing privacy risks throughout the development life cycle of a program or system.

"Security controls" means safeguards or countermeasures to avoid, detect, counteract or minimize security risks to physical property, information, computer systems or other assets.