TOPIC:

PROBOSED CYBER SECURITY STANDARDS

These are a set of guidelines or best practices that organizations can use to improve their cyber security posture.

Organizations use them to help them identify and implement appropriate measures to protect their systems and data from cyber threats.

They include:

1.ISOI IEC 27001: The International Organization for Standardization and the Electronical Commission.It includes requirements for developing an information security management system (ISMS) implementing security controls and conducting risk assessments.

It helps organizations manage their security practices in one place consistently and cost effectively.

2.NIST: it's created by the National Institute of Standard and Technology.

It assists organizations in managing and reducing cyber risks to critical infrastructure.it also helps organizations identify,assess and manage their cyber security risks in a structured and repeatable maner.

3.HIPAA: Health Insurance Portability and Accountability Act.It sets rules and standards for the protection of sensitive patient health information.It applies all forms of health information including paper records, electronic records and oral communications.

Aims at making it easier for people to keep their health insurance when they example change jobs, protect the confidentiality and security of health care information and help the health care industry control it's administrative costs.

4.FISMA:Fideral Information Security Modernization,provides a security framework for protecting federal government data and systems.

It requires federal agencies and their third parties to develop document and implement security policies and practices including the monitoring of their Information Technology infrastructure and conducting regular security audits.