

Enhances cryptography research and encourages the implementation of post-quantum cryptography standards throughout the United States.

Summary:

As quantum technology rapidly evolves, implementing security measures to protect our digital information and ensure a post-quantum future is essential. H.R. 3259, the Post Quantum Cybersecurity Standards Act, amends the National Quantum Initiative Act to direct the National Institute of Standards and Technology (NIST) to encourage the voluntary adoption of quantum-resistant cryptographic standards. NIST will achieve this goal by issuing guidance, assisting high-risk entities like critical infrastructure operators, and supporting a national transition to post-quantum security.

Additionally, H.R. 3259:

- Provides NIST the authority to help organizations strengthen their systems against quantum-era threats, in coordination with CISA and other federal and private-sector partners.
- Amends National Science Foundation research and development activities to include post-quantum cryptography in its cybersecurity research, ensuring continued innovation in encryption methods resilient to quantum and classical threats.

Background:

- The bill was offered as an amendment during the markup of the National Quantum Initiative Reauthorization Act during the 118th Congress and adopted by voice.
- This legislation aims to ensure that the United States is prepared for the challenges presented by advances in quantum computing technology, promoting a proactive approach to quantum cybersecurity.
- In 2024, NIST released a set of encryption tools designed to withstand the attack of a quantum computer.