COSMOS
Navigate the Compliance Universe

15 U.S. Code § 7432

National cybersecurity challenges

(a) Establishment of national cybersecurity challenges

(1) In general

To achieve high-priority breakthroughs in cybersecurity by 2028, the Secretary of Commerce shall establish the following national cybersecurity challenges:

(A) Economics of a cyber attack

Building more resilient systems that measurably and exponentially raise adversary costs of carrying out common cyber attacks.

(B) Cyber training

(i) Empowering the people of the United States with an appropriate and measurably sufficient level of digital literacy to make safe and secure decisions online.

(ii) Developing a cybersecurity workforce with measurable skills to protect and maintain information systems.

(C) Emerging technology

Advancing cybersecurity efforts in response to emerging technology, such as artificial intelligence, quantum science, next generation communications, autonomy, data science, and computational technologies.

(D) Reimagining digital identity

Maintaining a high sense of usability while improving the privacy, security, and safety of online activity of individuals in the United States.

(E) Federal agency resilience

Reducing cybersecurity risks to Federal networks and systems, and improving the response of Federal agencies to cybersecurity incidents on such networks and systems.