## Critical Infrastructure Protection

The need to protect the American cyber internet is important to inhibit the site after attacks from an unapproved person from accessing the sites. The attack was evidenced on September 11, 2001, this made the Americans realize the consequences of not protecting internet accessories from terrorists. The federal government thereby decided to input measures to protect the nation’s critical organization (Ref-J7X2B9). Head state, Obama issued Administrative Order 13636 that contains two policies, policy directive 21 and Resilience (PDD 21), the focus was to improve network security and the significant strategy to ensure total privacy by those handling the sites.

The federal government granted a critical substructure to be self-governing with defense from the National Intelligence that offered protection to the DOD workforces. In addition to that, in 2018, President Trump engaged in the computer security and Structure Security Agency to prevent the corporeal risk to the nation’s critical substructure. The government has regulated the liberty issues of the workers on the critical structure by imposing guidelines to monitor the operation of the critical organizations (Ref-AB1CD2). The government has regulated their operation of the cyber workforces through the annual evaluation of the sites' privacy in the respective departments to ensure no leakage of data shakes the National Security.

Yes, the balanced procedure first has to promote the consistent, vulnerable, and protected internet to nurture proficiency, invention, message, and commercial success regarding the critical organization while not interfering with privacy and the freedom of the civil liberties of the employees (Ref-DJ74KL). The policy should be just focused on the promotion of higher National Safekeeping improvement in consideration to the critical organization to prevent data leakage and not denying the employees the privacy and freedom to perform their duties on the security on the internet.