Cyber Compliance and Zero Trust

Carahsoft Federal Regulation Overview

Summary:

Zero Trust is defined by the NIST as the "term for an evolving set of cybersecurity paradigms that move defenses from static, network- based perimeters to focus on users, assets, and resources." In summary, zero trust employs the idea of "never trust, always verify" and treats everything as a suspected threat.

Zero Trust is one of the top cybersecurity priorities for state and federal agencies. The federal government has published multiple documents shaping compliance regulations for Zero Trust. This document demonstrates the the impact the policies and regulations that played a role in the creation of Executive Order 14028, M-22-01, M-22-09, CISA Cloud Security Reference, and CISA Zero Trust Maturity Model. In addition to the documents that played in impact, this overview illustrates which regulations and policies were enacted in response to the five aforementioned zero trust policies.

carahsoft

Technology by Policy

CYBERSECURITY