Zero Trust Architecture

Zero Trust Architecture is the gold standard to secure one or more networks controlled by a single corporation or entity. For example, Zero Trust:

- Reduces the risk of allowing insecure devices onto a network;
- Supports secure access to the network regardless of the location of the user or device;
- Adapts to a cloud-centric environment with flexible controls; and
- Improves compliance with data privacy and protection laws.

However, Zero Trust Architecture is not the ideal security solution for two or more co-equal branches of government to share the same network because, by definition, Zero Trust requires the administrator of one branch to hold the key to all the data and information of the other two branches.

The Legislature has at least four options.

Opt-in
Comply with Executive Zero Trust Policy
The Legislature could comply with the Executive Zero Trust policy.

If the Legislature made this decision, it would have no oversight of executive branch monitoring of its devices or systems. Nor would the Legislature be capable of preventing the executive from gaining access to all information and data on the Legislature's devices and servers, including pre-released audits, bill drafts, amendments, email content, and all other work products.

Negotiate New Parameters of the Zero Trust Policy
The Legislature could decide to comply with the Executive Zero Trust policy under certain conditions that have yet to be explored but would likely include conditions that the executive would not have access to legislative systems, devices, data, or information.

Opt-out
Not Comply with Executive Trust Policy but continue to use the Executive network
The Legislature could decide not to comply with Zero Trust. If the Legislature made this decision, the Executive could deny access to the executive network; or alternatively, establish more security controls resulting in additional authentication controls for end users. Additional controls could involve more stringent login requirements such as multi-factor authentication or having to repeatedly re-authenticate to a system.

Establish the Legislature's Own Network
Currently, the Legislature authorizes on ongoing appropriation of about $1,000,000 to SITSD for network services. The Legislature could use this money to off-set the price of establishing its own network. This option should not be considered without a complete cost estimate of owning a network. A preliminary review found no other state that shares a network with the Executive.