From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Control 3.13.7 feedback
Date: Tuesday, September 13, 2022 8:37:22 PM

800-171 rev 2 Control 3.13.7
Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

Maps to 800-53 SC-7(7)
800-53 rev4 text:
BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES
The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

800-53 rev5 text:
BOUNDARY PROTECTION | SPLIT TUNNELING FOR REMOTE DEVICES
Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using [Assignment: organization-defined safeguards].

The changes in 800-53 rev5 are helpful because they give companies the flexibility to allow split tunneling with company defined restrictions in place. Under 800-171 rev2, companies were unable to make decisions on how to allow split tunneling securely (such as by only allowing certain ports from the remote device). 800-171 rev3 should have sufficient flexibility in it to allow companies to determine what organization-defined safeguards should be in place.

Proposed updated text for Control 3.13.7
Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling) unless otherwise protected by alternative safeguards.