

[REDACTED]

From: V. Amira Armond [REDACTED]
Date: Friday, August 19, 2022 at 2:44:17 PM UTC-4
Subject: 3.1.20
To: 800-171comments@list.nist.gov <800-171comments@list.nist.gov>

3.1.20 – Verify and control/limit connections to and use of external systems.

[c] connections to external systems are verified;

[d] the use of external systems is verified;

The above assessment objectives for this practice are widely misunderstood in relation to AC-20(1), which I believe was the source of the word “verify”. Clarification should be added to the description, or to the practice itself, which makes it clear that the organization should verify that external systems meet their internally identified security requirements prior to allowing connections or use.

Potential re-write could be:

3.1.20 – Verify external systems meet organizationally defined requirements for cybersecurity and control/limit connections to and use of external systems.

[a] security requirements for external systems which have persistent connectivity to internal systems are identified;

[b] security requirements for external systems used to store, process, or transmit Controlled Unclassified Information are identified;

[c] security requirements are verified prior to allowing persistent connections to an external system;

[d] security requirements are verified prior to allowing the use of external systems;

V. Amira Armond

Kieri Solutions - Resilient IT

O: [REDACTED] M: [REDACTED]

*This email address is approved for communication up to Federal Contract Information (FCI).
For transfer of Controlled Unclassified Information (CUI) or higher, please contact me for
secure file transmission methods.*