Appendix 2a: Supplemental Certification Statement Document

BEAD Application

Cybersecurity and Supply Chain Risk Management Certification

The Virginia Office of Broadband has developed the following certification for entities seeking to deploy network facilities by utilizing funding through the BEAD program. This checklist focuses on the Cybersecurity and Supply Chain Risk Management requirements as described in the BEAD NOFO.

As a duly authorized representative of [Insert Applicant Name], I certify that the applicant:

1. Will submit a Cybersecurity Risk Management Plan to the Office of Broadband during the pre-contract phase that at minimum is:
    a. Operational, if the prospective subgrantee is providing service prior to the award of the grant; or
    b. Ready to be operationalized upon providing service, if the prospective subgrantee is not yet providing service prior to the grant award;
    c. Compliant with the latest version of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (currently Version 1.1) and the standards and controls set forth in Executive Order 14028 and specifies the security and privacy controls being implemented;
    d. Scheduled to be reevaluated and updated on a periodic basis and as events warrant; and
    e. Able to be resubmitted to the Office of Broadband within 30 days if the subgrantee makes any substantive changes to the plan

2. Will submit a Supply Chain Risk Management Plan to the Office of Broadband during the pre-contract phase that at minimum is:
    a. Operational, if the prospective subgrantee is providing service prior to the award of the grant; or
    b. Ready to be operationalized upon providing service, if the prospective subgrantee is not yet providing service prior to the grant award;
    c. Compliant with NIST publication NISTIR 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry* and related SCRM guidance from NIST, including NIST 800-161, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* and specifies the supply chain risk management controls being implemented;
    d. Scheduled to be reevaluated and updated on a periodic basis and as events warrant; and
    e. Able to be resubmitted to the Office of Broadband within 30 days if the subgrantee makes any substantive changes to the plan

3. Will obtain the above attestations from its network provider with respect to both cybersecurity and supply chain risk management practices if the applicant relies in whole or in part on network facilities owned or operated by a third party (*e.g.*, purchases wholesale carriage on such facilities.

Appendix 2a: Supplemental Certification Statement Document

Signature of Authorized Certifying Individual: _____
Titled of Authorized Certifying Individual: _____
Applicant Entity Name: _____
Date Submitted: _____

Notary:

I do hereby certify that _____ (Name of Authorized Certifying Individual), personally appeared before me and made oath that he/she is _____ (Title) of _____ (Applicant Entity Name) and that he/she is duly authorized to execute the foregoing document.

My commission expires: _____

Given under my hand this _____ (date) day of _____ (month), _____ (year).

Notary Public Signature: _____
Registration Number: _____