APPENDIX G

Alaska Broadband Grant Program

State of Alaska
Department of Commerce, Community, and Economic Development
Alaska Broadband Office

Part A: CYBERSECURITY RISK MANAGEMENT

Each Applicant for Connect Alaska funds from the State of the Alaska, Department of Commerce, Community & Economic Development, Alaska Broadband Office, must attest to the Cybersecurity Risk Management items below. Applicants must also obtain the below attestations from any network provider(s) who own or operate the network facilities relied upon by the Applicant.

By signing below, the Applicant attests to the following items:

1. (*Select One*)
   - ☐ *If the Applicant is already providing service*, a cybersecurity risk management plan is in place and operational.
   - ☐ *If the Applicant is not yet providing service*, a cybersecurity risk management plan is ready to be operationalized upon providing service.
2. The plan reflects or will reflect the latest version of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Cybersecurity and the standards set forth in Executive Order 14028[1].
3. If awarded, the plan will be submitted to the Alaska Broadband Office prior to finalization of the grant agreement and prior to any funds being disbursed to the subgrantee.
4. The plan will be reevaluated and updated periodically, or as necessary.
5. Updated plans will be submitted to the Alaska Broadband Office within 30 days of any substantive changes.

Under penalty of perjury, the undersigned official(s) certifies that official(s) is authorized to sign this certification, has read and understood the Applicant's required attestations, and that any information submitted in conjunction with these attestations is accurate and complete.

Part B: SUPPLY CHAIN RISK MANAGEMENT

Each Applicant for Connect Alaska funds from the State of the Alaska, Department of Commerce, Community & Economic Development, Alaska Broadband Office, must attest to the Supply Chain Risk Management items below. Applicants must also obtain the below attestations from any network provider(s) who own or operate the network facilities relied upon by the Applicant.

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

By signing below, the Applicant attests to the following items:

1. (*Select One*)
   - ☐ *If the Applicant is already providing service*, a supply chain risk management plan is in place and operational.
   - ☐ *If the Applicant is not yet providing service*, a supply chain risk management plan is ready to be operationalized upon providing service.
2. The plan is based on the NIST publication NISTIR 8276, Key Practices in Cyber Supply Chain Risk Management: Observations from Industry[2] and other related NIST guidance.
3. If awarded, the plan will be submitted to the Alaska Broadband Office prior to finalization of the grant agreement and prior to any funds being disbursed to the subgrantee.
4. The plan will be reevaluated and updated periodically, or as necessary.
5. Updated plans will be submitted to the Alaska Broadband Office within 30 days of any substantive changes.

Under penalty of perjury, the undersigned official(s) certifies that official(s) is authorized to sign this certification, has read and understood the Applicant's required attestations, and that any information submitted in conjunction with these attestations is accurate and complete.

DATED: _____
By: _____
Print Name: _____
Title: _____
Organization: _____

[2] https://csrc.nist.gov/pubs/ir/8276/final