Appendix A

Certification Regarding Compliance with Cybersecurity and Supply Chain Management Requirements

[To be completed and submitted by each applicant as part of its application]

On behalf of [*Organization Name*], I, [*print name*] _____, hereby certify that, in submitting this Tribal Broadband Connectivity Program (TBCP) application, my organization is in compliance with the Cybersecurity and Supply Chain Management requirements discussed in Section F.4 of the Tribal Broadband Connectivity Program Notice of Funding Opportunity, Funding Opportunity Number NTIA-ICG-TBCPO-2023-2008098, published on July 27, 2023. I further certify that my organization is in compliance with each of the below requirements and attest that:

My organization and any prospective or actual subgrantees of my organization fully recognize and understand that it is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cybersecurity threats. Entities receiving federal funds must therefore ensure that cybersecurity is integrated into the design, development, operation, and maintenance of critical infrastructure communication technology and operational technology;

In order to accomplish the cybersecurity objectives of the United States Government, my organization and any prospective or actual subgrantees will complete the following actions within twelve (12) months of the acceptance of any TBCP grant award to my organization:

1. Review the Cybersecurity and Infrastructure Security Agency (CISA) Cross-Sector Cybersecurity Performance Goals (CPGs) (https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf), which establish the baseline cybersecurity practices and controls with known risk-reduction value that are actionable and broadly applicable across all critical infrastructure sectors;

2. Perform an initial assessment of the cybersecurity practices of the TBCP award-funded project (Project) using the CISA CPG Checklist Adapted for Grant Awards. This assessment will include the cyber assets controlled as part of the execution of the Project and the cybersecurity practices of my organization and any parent and/or partner organizations;

3. Develop and submit a Cybersecurity Risk Mitigation Plan (Plan) for my organization and any prospective or actual subgrantees that includes:

a. The CISA CPG Checklist Adapted for Grant Awards with a current assessment documented for cyber assets controlled as part of the Project, as well as an assessment of the cybersecurity practices of my organization and any parent and/or partner organizations;

b. A prioritized list of Project CPG gaps that need to be addressed for cyber assets controlled as part of the execution of the Project, as well as any CPG gaps affecting my organization and any parent and/or partner organizations;

c. Documentation of Project cybersecurity risk mitigation efforts to be undertaken as part of the execution of the TBCP award, with a target implementation date identified for each mitigation effort, including mitigation efforts to address identified Project CPG gaps, as well as mitigation efforts to address identified CPG gaps of my organization and any parent and/or partner organization;

My organization and any prospective or actual subgrantees of my organization fully recognize and understand that any failure to submit and obtain the approval of a Plan by the National Telecommunications and Information Administration (NTIA) within twelve (12) months of acceptance of a TBCP award to my organization will result in corrective action, potentially including, but not limited to, the imposition of a performance improvement plan, additional risk monitoring measures, and/or possible limitations on certain uses of TBCP award funds;

With respect to Supply Chain Risk Management (SCRM), my organization has an SCRM plan (SCRM Plan or Plans) in place that is either: operational, if either my organization or any prospective or actual subgrantees is or are already providing any form or type of telecommunications services; or ready to be operationalized, if my organization and/or any prospective or actual subgrantees is or are not yet providing any form or type of telecommunications services;

The SCRM Plan is based upon the key practices discussed in the National Institute of Standards and Technology (NIST) publication NISTIR 8276, *Key Production 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;

The SCRM Plan will be reevaluated and updated by my organization on a periodic basis and as events warrant;

The SCRM Plan or Plans of any prospective or actual subgrantees will be submitted to my organization prior to the allocation of grant funds. If a prospective or actual subgrantee makes any substantive changes to its SCRM Plan, a new version will be submitted to my organization within 30 calendar days. My organization will provide its SCRM Plan and the SCRM Plan or Plans of any prospective or actual subgrantees to NTIA upon request; and

My organization will ensure that, to the extent that my organization and/or any prospective or actual subgrantee relies or rely in whole or in part on network facilities owned or operated by one or more third parties (*e.g.*, through the purchase of wholesale carriage on such facilities), my organization will obtain the above attestations from these third parties with respect to both cybersecurity and SCRM practices.

I understand and agree that, if I or my organization knowingly or negligently provides false or inaccurate information in this certification, the organization shall:

1. Not be eligible to receive the Tribal Broadband Connectivity Program grant funding associated with this certification and accompanying application for funding; and

2. Return any grant awarded under the Tribal Broadband Connectivity Program during the time that this certification was not valid; and

3. Not be eligible to receive any subsequent grants under the Tribal Broadband Connectivity Program; and

4. potentially be subject to criminal prosecution (including under 18 U.S.C. § 1001 and/or 1621), civil and administrative penalties, and other remedies, as may its officers, executives, members, or employees, as applicable, as well as any other associated entities, persons, or individuals, including I myself.

Signature of Authorized Organization Representative:

_____

Title: _____

Date: _____