Exhibit K: Cybersecurity and Supply Chain Risk Management Attestation

CNMI Broadband Equity, Access, and Deployment (BEAD) Program Subgrant Agreement between CNMI BPD and Micronesian Telecommunications Corp. dba IT&E

Field	Detail
Project Name(s)/Identifier(s)	All 20 Project Funding Areas (CNMI-S1 through CNMI-S17, CNMI-R1, CNMI-T1, and CNMI-T2 as individually detailed in the attached Exhibits A)
Subgrantee	Micronesian Telecommunications Corp. dba IT&E
BPD Subgrant Award Identifier	CNMI Broadband Equity, Access, and Deployment (BEAD) Program Subgrant Agreement (Covering all 20 PFA Awards)
Agreement Effective Date	May 13, 2026

Instructions: Pursuant to the Subgrant Agreement and the requirements of the Infrastructure Investment and Jobs Act (IIJA) (47 U.S.C. § 1702(g)(1)(B)) and the BEAD Notice of Funding Opportunity (NOFO) Section IV.C.2.c.vi, the undersigned Authorized Representative of the Subgrantee must attest below. This attestation and the underlying plans are required **prior to the allocation of any deployment funds** to the Subgrantee. These plans must ensure the **reliability and resilience** of the broadband infrastructure, particularly against threats such as **natural disasters** (e.g., typhoons).

A. Cybersecurity Risk Management Plan Attestation

The Subgrantee hereby attests that:

1. The Subgrantee has a cybersecurity risk management plan (the plan) in place that is either **operational** or **ready to be operationalized** upon providing service.
    a. (Indicate status: [Operational / Ready to be Operationalized])

2. The plan reflects 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** (Improving the Nation's Cybersecurity). The plan specifies the security and privacy controls being implemented.
3. The plan will be **reevaluated and updated on a periodic basis and as events warrant**.
4. The plan **has been submitted, or will be submitted, to CNMI BPD** prior to the first allocation of Subgrant funds for deployment activities. If the Subgrantee makes any **substantive changes** to the plan, a new version will be submitted to CNMI BPD within **30 days**.

B. Supply Chain Risk Management (SCRM) Plan Attestation

The Subgrantee hereby attests that:

1. The prospective Subgrantee has an SCRM plan in place that is either **operational** or **ready to be operationalized**.
    a. (Indicate status: [Operational / Ready to be Operationalized])
2. The plan is based upon the key practices discussed in **NISTIR 8276** (Key Practices in Cyber Supply Chain Risk Management: Observations from Industry) and related SCRM guidance from NIST, including **NIST Special Publication 800-161** (Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations). The plan specifies the supply chain risk management controls being implemented.
3. The plan will be **reevaluated and updated on a periodic basis and as events warrant**.
4. The plan **has been submitted, or will be submitted, to CNMI BPD** prior to the allocation of funds. If the Subgrantee makes any **substantive changes** to the plan, a new version will be submitted to CNMI BPD within **30 days**.

C. Third-Party Network Reliance

The Subgrantee further attests that **to the extent it relies in whole or in part on network facilities owned or operated by a third party** (e.g., purchases wholesale carriage), the Subgrantee has obtained **equivalent attestations** from that network provider regarding their compliance with cybersecurity and SCRM practices. Copies of these third-party attestations will be provided to CNMI BPD upon request.

D. Certification

I, the undersigned authorized representative of the Subgrantee, hereby certify that the attestations made in Sections A, B, and C (if applicable) of this Exhibit K are true, accurate, and complete to the best of my knowledge and belief as of the date signed below. The Subgrantee understands that these attestations are **material representations of fact** upon which CNMI BPD will rely, and that failure to comply with these statutory requirements, or the failure to maintain network **reliability and resilience**, may result in remedies up to and including **termination of the Agreement and recoupment/clawback of funds**.

For Micronesian Telecommunications Corp. dba IT&E:

By: (Signature) _____

Printed Name: David H. Gibson

Title: CEO

Date: _____