UNDERSTANDING AND MEETING THE NEW CYBERSECURITY AND SCRM REQUIREMENTS FOR THE BEAD PROGRAM

State and Territory Governments Guide to Meeting New Cybersecurity and Supply Chain Risk Management Requirements from NTIA Notice of Funding Opportunity (NOFO)

NEW SECURITY REQUIREMENTS

NTIA has established new and unprecedented Cybersecurity and Supply Chain Risk Management (SCRM) requirements in its Notice of Funding Opportunity for subgrantees to be eligible for funding from the Broadband Equity Access Deployment (BEAD) program.

States and territories must review the Cybersecurity and SCRM Plans from prospective subgrantees (e.g., service providers) before allocating any BEAD program funds to ensure they meet the NTIA grant requirements.

States and territories will require prospective subgrantee's attestation that the proper plans are in place and make the subgrantee's Cybersecurity and SCRM plan available to NTIA upon request.

> *A prospective subgrantee must attest that:*
>
> *It has a Cybersecurity and SCRM plan in place that is either: a. operational, if the prospective subgrantee is already providing service at the time of the grant; or b. ready to be operationalized, if the prospective subgrantee is not yet providing service at the time of grant award.*
>
> **- NTIA's Notice of Funding Opportunity**

WHY THIS IS SIGNIFICANT

- It is the first time Cybersecurity and SCRM Plans are required for federal funding
- Requirements include baseline cybersecurity and SCRM guidelines, measures, and controls documents
- Attestation that the Cybersecurity and SCRM plans are correct, true, and genuine in meeting the baseline requirements set forth in the NIST publications and Executive Order 14028

BASELINE SUPPLY CHAIN RISK MANAGEMENT AND CYBERSECURITY REQUIREMENTS CAN BE FOUND IN:

Supply Chain Risk Management

- NIST publication NISTR 8276, *Key Practices in Cyber Supply Chain Risk Management Observations from Industry*, and related SCRM guidance from NIST
- NIST 800-161, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* and specifies the supply chain risk management controls being implemented

Cybersecurity

- Cybersecurity: NIST Framework for Improving Critical Infrastructure Cybersecurity
- Cybersecurity: Standards and controls set forth in U.S. Executive Order 14028

PRESCRIPTIVE MEASURES

The Infrastructure Act directs the Assistant Secretary to specify prudent Cybersecurity and supply-chain risk management practices for subgrantees deploying or upgrading broadband networks using BEAD funds.

- NTIA's Notice of Funding Opportunity

ALIGNMENT WITH BEAD SECURITY REQUIREMENTS

TIA QuEST Forum's Supply Chain Security Standard, SCS 9001, is independently certified and can be used to demonstrate alignment with the Cybersecurity and SCRM requirements defined in the BEAD Notice of Funding Opportunity.

SCS 9001 CERTIFICATION DELIVERS:

A clear checklist of requirements demonstrating the necessary controls and measures are in place to meet the baseline Cybersecurity and SCRM requirements for the BEAD NOFO. A process to collect data to publish anonymous benchmarking reports and defines industry best-in-class, average and worst-in-class performance metrics. This valuable data ensures continuous improvement in supply chain security processes and best practices. An on-going Cybersecurity and SCRM supply chain security measure improvement process that requires 3-year re-certification and periodic surveillance audits in alignment with the NOFO Cybersecurity and SCRM requirements that plans shall be "reevaluated and updated on periodic basis."

FOR MORE INFORMATION AND UPDATES VISIT TIAONLINE.ORG/U-S-BEAD-PROGRAM

CONTACT US TODAY TO LEARN MORE ABOUT HOW SCS 9001 CERTIFICATION MEETS THE CYBERSECURITY AND SUPPLY CHAIN SECURITY RISK MANAGEMENT REQUIREMENTS IN THE BEAD NOFO AT SUPPLYCHAINSECURITY@TIAONLINE.ORG