Virginia Office of Broadband

BEAD Application Requirements Overview

Cybersecurity and Supply Chain Risk Management
Section 2.16.4

Section 2.16.4 Cybersecurity and Supply Chain Risk Management Summary

1 DESCRIPTION: WHAT?

- Section IV.C.2.c.vi of the BEAD Notice of Funding Opportunity (NOFO) requires both:
  1. Cybersecurity risk management and;
  2. Cybersecurity supply chain risk management practices (C-SCRM)
- Must be operationalized *or* be ready to be implemented prior to any fund allocations being awarded to a subgrantee

2 RATIONALE: WHY?

- To ensure subgrantees identify and manage their cybersecurity and third party risks.

3 ROLES AND RESPONSIBILITIES: WHO?

Applicant: Demonstrate an understanding of and compliance with Section 2.16.4 requirements

DHCD Office of Broadband: Evaluate applications

4 DESCRIPTION: HOW?

Subgrantees should submit these Plans to the Office of Broadband prior to the allocation of funds. The Office of Broadband must provide the plans to NTIA upon NTIA's request.

5 QUESTIONS?

Contact: broadband@dhcd.virginia.gov

Additional Resources: https://www.dhcd.virginia.gov/bead

6 ROADMAP: WHEN?

Milestone	Phase
Applicant to document their Plans to comply with NOFO requirements (may use Plan templates provided by Virginia to develop); evaluate Plans using checklist.	Application
Applicant to submit Cybersecurity Risk Management Plan to the Office of Broadband.	Application
Applicant to submit C-SCRM Plan to the Office of Broadband.	Application
The Office of Broadband to submit Cybersecurity Risk Management Plan and C-SCRM Plan to NTIA	Upon Request

Section 2.16.4 Cybersecurity and Supply Chain Risk Management Breakdown

1. Cybersecurity and Supply Chain Risk Management

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.

WHAT IS THE ASK?

Each applicant must maintain, operationalize, and submit to the Office of Broadband the following plans:
(1) a cybersecurity risk management plan and
(2) a cyber supply chain risk management (C-SCRM) plan.

WHAT ARE THE REQUIREMENTS?

Both plans must be:

- Operational or ready to be operationalized
- Re-evaluated at defined intervals and as events warrant
- **The cybersecurity risk management plan must:**
- Align to the latest version of the NIST Cybersecurity Framework (CSF)
- Meet standards set forth in Executive Order 14028

The cyber supply chain risk management plan must:

- Be based on key practices discussed in NISTIR 8276 *"Key Practices in Cyber Supply Chain Risk Management (SCRM): Observations from Industry"*
- Be based on related SCRM guidance from NIST 800-161 *"Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations"*
- Specify the controls to be implemented

WHAT STEPS SHOULD BE TAKEN?

- Applicant may leverage plan templates and plan checklists to accelerate their documentation of the Plans.
- Office of Broadband certifies that the Plans meet NOFO requirements.
- (*If the subgrantee relies in whole or in part on network facilities owned or operated by a third party)* Office of Broadband obtains attestations from network provider with respect to cybersecurity and supply chain risk management practices.

Section 2.16.4 Cybersecurity and Supply Chain Risk Management Actions

The applicant is expected to complete the following task(s) to satisfy the requirements for Section IV.C.2.c.vi which are laid out on Pages 70-71 of BEAD NOFO and adopted by the Office of Broadband on Pages 56-57 of their Initial Proposal Volume 2. The Office of Broadband has developed a template and checklist for the Cybersecurity and C-SCRM plans to assist applicants in the process.

REQUIREMENTS

The Office of Broadband posted the requirement specifics in IPv2

Fall 2023

APPLICATION

Applicant to include all documentation, narratives, and certifications in the application

During Application

PRE-CONTRACT

In the Post-Award but Pre-Contract phase, awardees may be asked to provide additional information

2025

SUBGRANTEE MONITORING

The Office of Broadband will monitor subgrantees to ensure compliance with ongoing requirements for this section

Ongoing