Broadband Infrastructure PLAYBOOK

Implementing BEAD and other Broadband Deployment Programs

VERSION 3.0 (2023)

Cybersecurity and Supply Chain Risk Management Under the BEAD Program

The Notice of Funding Opportunity ("NOFO") released by the National Telecommunications and Information Administration ("NTIA") requires each Eligible Entity to ensure that prospective subgrantees of Broadband Equity, Access, and Deployment ("BEAD") funding attest that they meet certain cybersecurity and supply chain risk management requirements. These requirements are often combined into a single Cybersecurity and Supply Chain Risk Management Plan (C-SCRM Plan).

We summarize below the NOFO's cybersecurity and supply chain risk management baseline requirements to which prospective subgrantees must attest and then provide recommendations on how Eligible Entities can work with subgrantees to meet these requirements.

NOFO Cybersecurity Baseline Requirements:

1. The prospective subgrantee has a cybersecurity risk management 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.

2. The plan reflects the latest version of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (formerly known as the NIST Cybersecurity Framework or NIST CSF; the current version is 1.1) and the standards and controls set forth in Executive Order 14028 and specifies the security and privacy controls being implemented.[1]

3. The prospective subgrantee will reevaluate and update the plan on a periodic basis and as events warrant.

4. The prospective subgranteee will submit the plan to the Eligible Entity prior to the allocation of funds. If the subgrantee makes any substantive changes to the plan, it will submit a new version to the Eligible Entity within 30 days.

NOFO Supply Chain Risk Management (SCRM) Baseline Requirements:

1. The prospective subgrantee has a 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;

1 Eligible Entities should be aware that NIST is in the process of updating this Framework and has released draft v. 2.0 for public comment.

2. The plan is based upon the key practices discussed in the NIST publication NISTIR 8276, Key Practices 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;

3. The prospective subgrantee will reevaluate and update the plan on a periodic basis and as events warrant; and

4. The prospective subgrantee will submit the plan to the Eligible Entity prior to the allocation of funds. If the subgrantee makes any substantive changes to the plan, prospective subgrantee will submit a new version to the Eligible Entity within 30 days.

The NOFO also states that an Eligible Entity must ensure that, to the extent a BEAD subgrantee relies on network facilities owned or operated by a third party (e.g., purchases wholesale carriage on such facilities), the subgrantee obtains attestations from its network provider with respect to both cybersecurity and supply chain risk management requirements. An Eligible Entity may propose to NTIA additional measures that it deems are necessary to safeguard networks and users.

Recommendations for Eligible Entities to Support Prospective Subgrantees:

- Proactively offer stakeholders educational opportunities about the NIST Framework.
- Permit each subgrantee to combine its Cybersecurity Plan and its Cyber Supply Chain Risk Management plan in a single document (i.e., a C-SCRM Plan).
- Develop a process for collecting and maintaining copies of subgrantee plans.
  - Given the significant security risks that can arise from unauthorized access and review, ensure that plans can be submitted and maintained confidentially and will not be included in any public posting of applications or subject to any Freedom of Information Act (FOIA) requests.
- Encourage subgrantees to stay abreast of current cyber threats and mitigation measures through membership in a relevant ISAC (information sharing and analysis center), participation in Cybersecurity and Infrastructure Security Agency's (CISA) Automated Indicator Sharing (AIS), or other sufficient means.
- Because each cybersecurity risk management plan is specific to a company and cannot be judged in comparison to any other plan, not include the content of a plan as part of criteria to score deployment applications.