[Title:] Are you ready to meet BEAD cybersecurity requirements?

[Subtitle:] What you need to know

[Client:] XYZ Solutions

Local governments and the broadband industry are eagerly anticipating the launch of a new grant opportunity: the Broadband Equity, Access, and Deployment (BEAD) Program. The BEAD Program—which is part of the Infrastructure Investment and Jobs Act of 2021 (IIJA, which is also called the Bipartisan Infrastructure Law)—ensures a minimum of $100 million for each U.S. state and $25 million for each U.S. territory for the creation and deployment of broadband networks. This is exciting news for those who need and those who supply broadband.

Now is the moment to start preparing for the Program's prerequisites. The BEAD Program's Notice of Funding Opportunity (NOFO) includes strict cybersecurity requirements, for which it offers two primary reasons: "(a) protecting American communications networks and those who use them from domestic and international threat actors, and (b) promoting the natural evolution of cybersecurity and supply-chain risk management practices in a manner that allows flexibility in addressing evolving threats." The importance of these two reasons for the cybersecurity requirements is self-evident; cybersecurity is simply a must in a connected world in which a lack of proper protective measures can have dramatic consequences.

Let's delve more deeply, then, into the Program's cybersecurity requirements. The BEAD NOFO includes four provisions:

1. The entity applying for BEAD funding must have a cybersecurity risk management plan in place that is either operational or "ready to be operationalized upon providing service."
2. The plan must adhere to the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity. (More about this requirement in a moment.)
3. The cybersecurity plan must be reassessed and updated regularly.
4. The plan—and any changes to it—must be submitted before BEAD Program grant funds will be allocated.

Though all four of these requirements must be met, the second is the area where the rubber hits the road. The NIST Framework for Improving Critical Infrastructure

Cybersecurity—full text of the current version found here—is a comprehensive, 55-page document intended to help organizations:

1. "Describe their current cybersecurity posture;
2. Describe their target state for cybersecurity;
3. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4. Assess progress toward the target state;
5. Communicate among internal and external stakeholders about cybersecurity risk."

The Framework Core includes several benchmarks you must meet to have an adequate cybersecurity plan (and, therefore, to be eligible for BEAD Program funding). Here's a summation of what the NIST Framework requires for an adequate cybersecurity plan:

- A full asset management plan that reviews devices, systems, data, and staff to identify cybersecurity risks
- An evaluation of your business' governance, mission, objectives, and stakeholders to ensure proper prioritization of cybersecurity
- A complete risk assessment and risk management strategy
- A supply chain risk management (SCRM) strategy to address risks related to suppliers and other third parties
- Implementation of identity management and authentication controls to limit and vet your system's users
- Deployment of cybersecurity training for your staff and your partners
- A functioning data security platform that protects the confidentiality and integrity of your data
- Creation of security policies to protect your data along with a plan to enforce those policies
- Application of technology that actively protects your data and other systems
- A system for continuous monitoring and detection of security anomalies, issues, or major events
- A written process for how and by whom a cybersecurity event will be handled
- Demonstration of the ability to respond to cybersecurity incidents and communicate about them as needed, both internally and externally
- A detailed set of steps for analyzing cybersecurity incidents when and after they occur, and mitigating future incidents
- Processes and procedures to recover data or systems as needed, including communication with internal and external parties about the recovery status

- A plan for the ongoing maintenance of your information systems, including the ability to improve response and recovery time after an incident

The amount of detail required by the BEAD Program and the NIST Framework for your cybersecurity plan can seem daunting, especially since it's just one of the many standards that must be met when applying for a BEAD grant. Don't approach it alone. As you prepare to meet the BEAD Program grant application requirements, finding a partner with extensive cybersecurity experience who can help you meet the NIST Framework benchmarks is vital. The BEAD funding season will be here before you know it—now is the time to start the conversation with an expert in managed services, data privacy, and compliance solutions—a partner like XYZ—who can help you meet these extensive requirements.