The Arkansas State Broadband Office (ASBO) is dedicated to ensuring the protection of sensitive and proprietary information submitted during the application process. To provide transparency and assurance to applicants, our trusted vendor partners, Michael Baker International, Boston Consulting Group (BCG), and Ready.net, have submitted detailed statements below outlining their measures for safeguarding all confidential data.

These efforts are designed to assure applicants that their submissions will be protected with the highest standards of data security.

Prospective applicants should also refer to NTIA's BEAD Notice of Funding Opportunity (NOFO), pages 94-95, for information concerning how the U.S. Department of Commerce will handle protected and proprietary information related to the BEAD program.

From Michael Baker International:

Michael Baker International, its employees, consultants, and contractors ("MBI") will take reasonable measures to safeguard information clearly marked by the applicant as protected, proprietary, or confidential information, including personally identifiable information ("Confidential Information"), obtained through the grant pre-qualification, application, award, administration, and enforcement process, consistent with applicable law. Except as required by applicable laws, rules, regulations, and legal requirements, MBI will not use or disclose any Confidential Information for any purpose other than for the performance of its grant-related obligations on behalf of the State of Arkansas. Confidential Information will only be shared with employees, consultants, and contractors with a need to know such information for performing those obligations.

MBI may be required to submit financial and performance information and data to the Department of Commerce and/or other federal agencies, employees, and contractors, as necessary to comply with the Notice of Funding Opportunity and other applicable laws, rules, regulations, and legal requirements.

From Ready.net:

Ready uses a multi-tenanted data model that secures customer data via a uniquely identifiable internal tenant id. This allows us to logically segregate SBO and other data, secure it in our logic tier, and identify/sanitize any tenant data if the need arises.

When data is at rest, it is stored via RSA 128-bit encryption. In transit, our data is sent using encrypted TLS (SSL) 1.2+. Our internal data systems are accessible via secure VPN. All external systems have certificates granted from Google Trust Services LLC - https://pki.goog - or from Amazon Trust Services - https://www.amazontrust.com/repository/. Internal systems have certificates signed using an internal certificate authority, which also uses RSA 128-bit encryption.

We rely on our cloud service providers in AWS and GCP to implement further security measures around the hardware of the systems themselves. In terms of our cloud usage, we regularly review and tighten our firewall policies across our cloud infrastructure. We have implemented continuous vulnerability and intrusion detection + scanning according to SOC2 recommendations, as well as robust logging + monitoring across our production infrastructure. We have regular penetration testing, security audits, and a paid bug bounty program too.

From Boston Consulting Group:

Boston Consulting Group ("BCG") maintains strict procedural and technical protocols to ensure that the information shared by each client is kept secure and confidential. In order to properly maintain client confidential information and prevent any conflicts of interest, BCG operates under stringent policies and guidelines which include the following: (i) BCG adheres to strict confidentiality obligations with its clients and ensures that each BCG consultant is trained to abide by these obligations and our internal procedures; (ii) Each individual client team establishes confidential "firewalls" between itself and other client teams working in the same industry and/or practice group (and the rest of the company and all third parties),so that no information is shared between competitor groups or with unauthorized individuals or entities; (iii) BCG fosters (to the extent possible) geographic/physical separation among BCG client teams working with competitive companies in the same industry; and (iv) BCG employs technical security and encryption protocols to ensure all confidential information is safeguarded securely from inadvertent disclosure of any kind.

BCG maintains a best-in-class IT system environment to meet special safeguarding and privacy requirements, ensuring that nonpublic information is not accessed by unauthorized personnel. This separation is continually monitored. Only BCG employees assigned to a specific contract have access to project information. Other BCG employees, regardless of their roles or clearances, do not have access to this data. Client documents are managed in central folders with limited access rights, protected through encryption, complex passwords, access controls, and data loss protection protocols. BCG has implemented security measures to detect and prevent unauthorized access to equipment and data storage devices, including restrictions on email attachments for external correspondence.