Cybersecurity Risk Management Plan Compliance for BEAD

Overview

All BEAD subgrantees must have an operational cybersecurity risk management plan prior to signing subgrantee agreements. The plan must be in compliance with federal cybersecurity guidance and should be reevaluated on a periodic basis. Subgrantees must share their plan with UBC prior to fund allocation, and must resubmit the plan to UBC within 30 days of any substantive changes.

NIST Framework for Improving Critical Infrastructure Cybersecurity

Identify   Protect   Detect   Respond   Recover

The NIST Framework includes current and target organizational profiles. These profiles characterize risk management objectives the organization currently achieves and outcomes to be prioritized. The Framework also organizes cybersecurity risk governance into four tiers, from Partial to Adaptive. These tiers reflect the rigor of an organization's risk management practices and the processes in place to manage risk. It is recommended that organizations advance tiers as cybersecurity risks are identified.

Executive Order 14028

- Includes sections such as:
  - Enhancing software supply chain security
  - Improving detection of cybersecurity vulnerabilities and incidents
  - Improving investigative and remediation capabilities

- Based on this Executive Order, NIST has identified criteria to evaluate software security; criteria to evaluate security practices of developers and suppliers; and tools to demonstrate conformance with secure practices.

- These criteria and tools are available for use and can be accessed at NIST's website.

CONNECTING UTAH