Cybersecurity & BEAD:

Steps to Comply

Presented By

Guide Star

A Division of CCI Systems

GUIDE STAR

A division of CCI Systems, Guide Star is an IT-managed service provider specializing in technical and end user support, monitoring, and security for small to mid size business and internet service providers across the US and Canada.

CCI systems®

Guide Star
A Division of CCI Systems

EVAN RICE

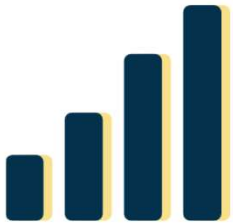
An experienced IT executive with a focus on cyber security and operational excellence, Evan serves as the Senior Vice President of Guide Star, a division of CCI Systems. He is an industry advisor for programs at Michigan Technological University and Dickinson-Iron ISD. Evan has been with CCI Systems / Guide Star for over 10 years.

PLAN

CONTROL FAMILIES

- Identify, Protect, Detect, Respond, Recover, **AND** Supply Chain
- Holistic approach covering the entire cybersecurity lifecycle.

ADVISORY PROCESS



- Work with our experts through a maturity model grading.
- Map current processes to compliance controls, even if undocumented.

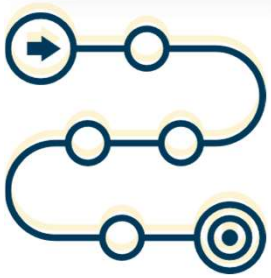
PLAN

FUTURE STATE PLANNING

POLICY AND PROCEDURE ALIGNMENT

- Define your intended future state for policies and procedures.
- Comprehensive documentation for strategic alignment.

GAP ANALYSIS AND COST ESTIMATION



- Identify compliance gaps and estimate associated costs.
- Ensure a clear roadmap for necessary improvements.

Deliverables: Written Information Security Program | Documented List of Gaps | Cybersecurity Compliance Roadmap | Budget

SUBMIT

- **Take your cyber plan and combine it with the other plans:**
  - Architecture
  - Construction
  - Permitting
  - Rollout
- **Submit to your State Broadband Authority**

- **You can earmark BEAD funds for implementation of the cyber controls**
  - Adding staff
  - Purchase software
  - Network software upgrades, including cybersecurity solutions
  - Training for cybersecurity professionals who will work on BEAD-funded networks
  - Potentially Subject Matter Expert (SME) consultation

BUILD

You must communicate with your technology team the things you've built into your plan

- **Parallel project plan for cybersecurity components** that goes along with your construction plan and rollout and expansion of your core network
  - **Needs to include 3 aspects of cybersecurity**
    - Hardware
    - Software
    - People
- Prove you've eliminated gaps identified during the planning phase – **must have compliance program**
- Understand what the final state needs to be for the 3 aspects
  - How to deploy these things and having 3rd party resources to help deploy on time

Deployment Examples:

- Firewall and DDoS predict protection
- Security, incident event monitoring
- CVM software
- MFA

MAINTAIN

- **Be ready to perform attestations**
- **Most states for NIST will have future anticipation of when you have to re-attest**
  - Will ask if there's significant change to the network, cybersecurity control policy or procedure, etc.
- **Must have compliance program that proves you are doing the things ongoing**
- **Must have ongoing standards for:**
  - Patching
  - CVE
  - Access Control Logging
  - SIEM

Red vs. Blue vs. Green Teams

Proactive experts identify vulnerabilities and provide expert guidance on regulations and emerging threats.

Reactive experts eliminate the risks the red team identifies and manage security operations across the business.

Compliance experts that know how to look at a business processes and determine if the protections in place are adequate and being used appropriately.

CONCTACT

Evan Rice

evan.rice@guide-star.com

www.guide-star.com

Guide Star

A Division of CCI Systems