Washington Update

Oct. 24, 2023
Jill Canfield
General Counsel, VP of Policy
Jcanfield@ntca.org

NTCA THE RURAL BROADBAND ASSOCIATION®

Regulatory issues/priorities

Universal Service Fund

- ACAM Elections
- Future of the fund

Digital Discrimination

BEAD

Cybersecurity

Open Issues - Support

Enhanced ACAM (Alternative Connect America Cost Model)

- Optional(new)funding mechanism in exchange for (new) build out obligations
  - Longer support if build to higher speed, 100% build out
- Tied to not yet finished broadband maps – support may fluctuate
- Unelect?

Future of USF

Much focus and $ devoted to building, what about sustainability?

Dwindling contribution base

Series of positive bills (no traction)

Net Neutrality rulemaking

- If classify Broadband as a telecom service, would need to contribute
  - BUT FCC choosing to forbear with no explanation

Court Challenge!

Adoption, Equity & Inclusion

Adoption, Equity & Inclusion

- Affordable Connectivity Program
  - Implementation
  - Appropriations
- Lifeline
  - Future Applications/Relevance
  - Voice Subsidy
- Digital Equity Planning and Use
  - Affordability Measures

BEAD

Key Questions Include:

- What is a “High-Cost” Area for Matching? (F)
- What is “Extremely High-Cost” for Overriding of Fiber Priority? (S)
- State Challenge Processes (F → S)
- Scope of “low-cost option” and “affordability”? (S)
- Buy American and other Supply Chain Issues? (F)
- Part 200 (F)
- Scoring rubrics (S)

Cybersecurity

Why should you pay attention to cybersecurity?

Protect your networks and assets

The federal government is imposing regulations

Financial incentive

300,000 malware created daily

27% of malware breaches involve ransomware

Ransomware top cause of financial loss in SMEs

Legal and regulatory “incentives”

- SEC rules on risk management, strategy, governance in incident response disclosure
- Cyber Incident Reporting for Critical Infrastructure Act
- FCC breach notification changes
- Government funding tied to cybersecurity requirements (EACAM, BEAD)

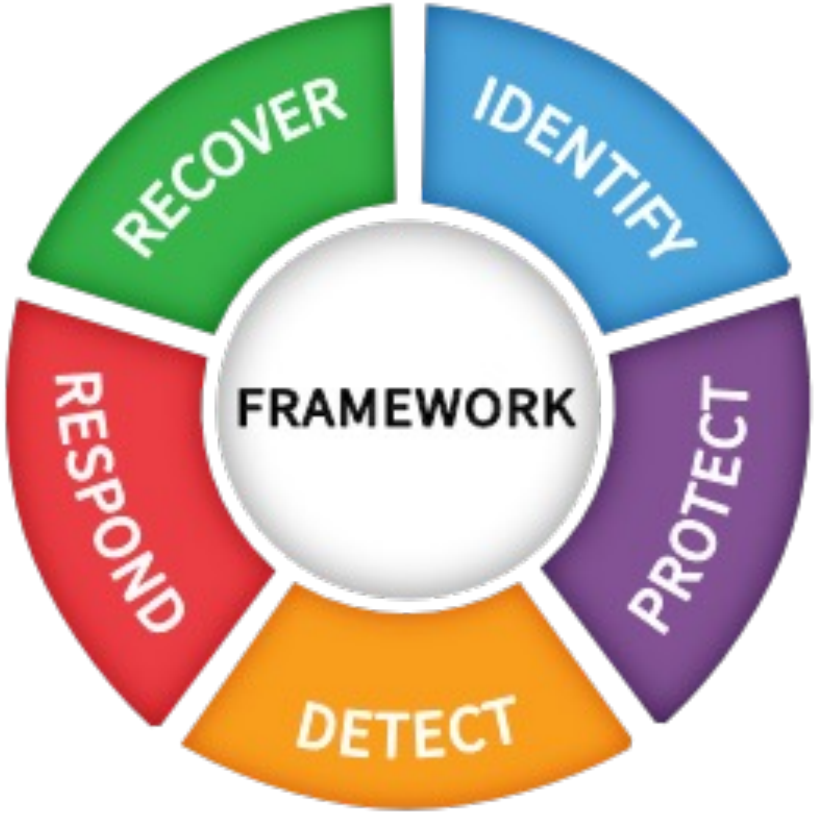
E- ACAM Cyber Requirements

- Implement by Jan 1, submit to USAC by Jan. 2
- Reflect NIST Framework
- Reflect best practices (CISA Cross-Sector Performance Goals and Objectives)
- Incorporate Supply Chain Risk Management
- Submit substantive modifications to plan

BEAD Cyber Requirements

- Attest that will have plan when apply for funds
- Submit plan to State before allocation of funds
- NTIA may request from the State
- Based on NIST Cybersecurity Framework
- Incorporate Supply Chain Risk Management Guidance
- Submit changes

NIST Cybersecurity Framework



Identify

Organizational understanding of assets

Cybersecurity policies

Risk management team

Contracts with third parties require notification

Participation in information sharing forum

CyberShare®

The Small Broadband Provider ISAC

Sign up: https://www.cyber-share.org/

Protect

What safeguards do you have to ensure delivery of critical services?

- Manage IDs and credentials
- Password change policy
- Limit access to property, systems
- Train users
- Use MFA, Network Segmentation, Encryption
- Do backups and patches according to schedule

```
irror_mod = modifier_ob.
t mirror object to mirror
irror_mod.mirror_object
peration == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
_operation == "MIRROR_Y":
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
_operation == "MIRROR_Z":
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

election at the end -add
_ob.select= 1
er_ob.select=1
ntext.scene.objects.activ
("Selected" + str(modifier
irror_ob.select = 0
 bpy.context.selected_obj
ata.objects[one.name].sel

int("please select exactl

-- OPERATOR CLASSES ----

types.Operator):
 X mirror to the selected
ject.mirror_mirror_x"
rror X"

ontext):
ext.active_object is not
```

Detect

- How do you discover a security event?
- Monitor access to building, sensitive information, email
- Monitor network for intrusions

Respond

- How do you respond to a security event?
  - Do you have a written incident response plan (yes!)
  - Cybersecurity insurance
  - Do you remove user access, remove access to devices
  - Policy to report to relevant organization (CISA)
  - Vulnerability scanning

Recover

What will you do after an event?

What is your plan for recovering and restoring service or access

How will you communicate event and response internally/externally

NIST 2.0

NIST
National Institute of
Standards and Technology

Not an overhaul of Cybersecurity Framework

Will add (pull out to highlight) governance function

More specific information about supply chain risk management

Additional requirements

- Supply Chain Risk Management
  - not a separate document, incorporate into your cybersecurity plan

- Cross-Sector Cybersecurity Performance Goals
  - Baseline set of best practices with known risk-reduction value
  - Aligns with NIST Cybersecurity Framework

Questions?

Jill Canfield

jcanfield@ntca.org

www.cyber-share.org

Google: NTCA + cybersecurity series