Cybersecurity for BEAD & Other Funding

BEAD, E-ACAM, ReConnect

September 2023

How You Can Prepare Yourself for the Upcoming Funding Opportunities

WTA – Fall Conference

VantagePoint
EMPLOYEE OWNED

About the Presenter

Andy Deinert

- Director of Network and Security Services
  - Cybersecurity
  - Routing / Switching
  - Managed Services
- Andy.Deinert@vantagepnt.com

FEASIBILITY & FUNDING

NETWORK DESIGN & ENGINEERING

OSP & NETWORK IMPLEMENTATION

CYBERSECURITY & DATA NETWORKING

REGULATORY COMPLIANCE

OPERATIONS & STRATEGY

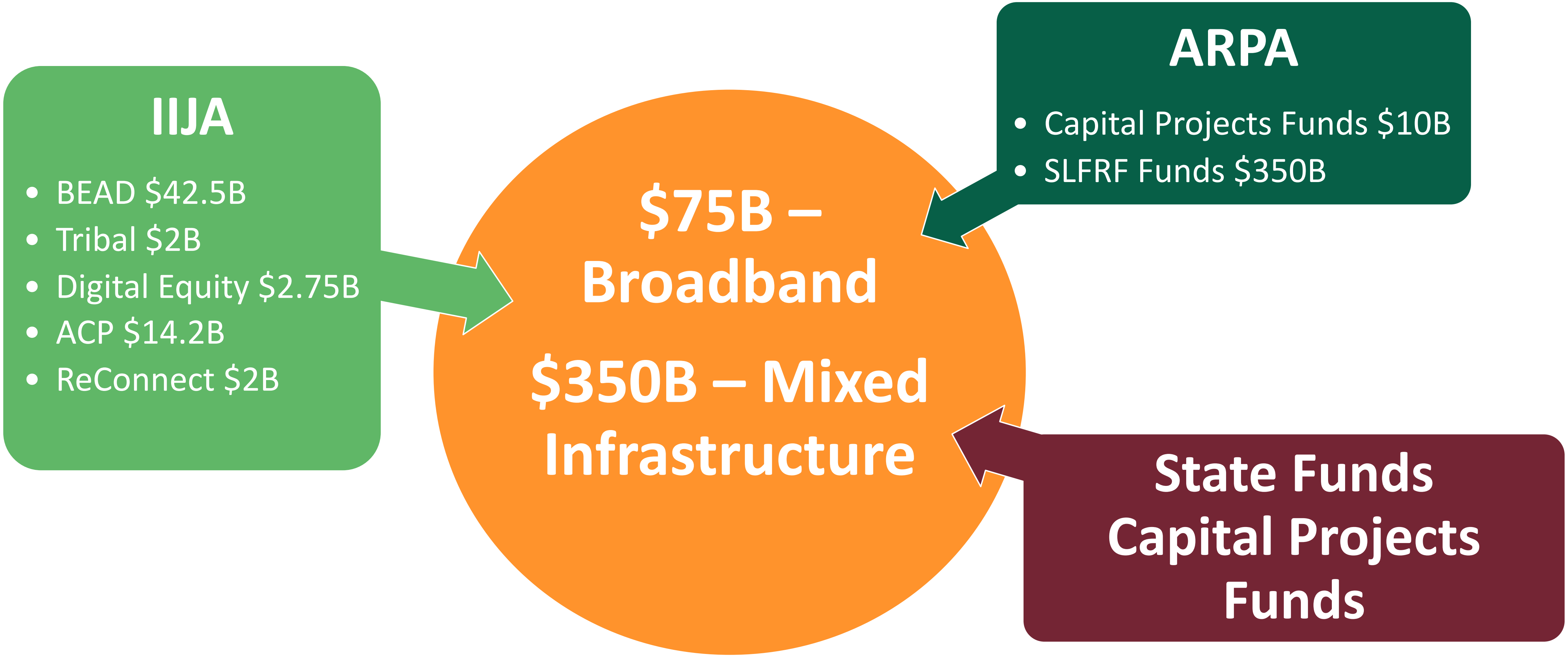
VOICE, VIDEO, DARK FIBER & MORE

Start-to-FUTURE Solutions under one roof.

Better broadband means better lives. Vantage Point helps clients deliver on that promise through start-to-finish engineering and consulting services. Our solutions are customized to meet your unique needs and goals from due diligence to deployment – **and beyond.**

VantagePoint

Available Funding



IIJA

- BEAD $42.5B
- Tribal $2B
- Digital Equity $2.75B
- ACP $14.2B
- ReConnect $2B

ARPA

- Capital Projects Funds $10B
- SLFRF Funds $350B

State Funds Capital Projects Funds

$75B – Broadband

$350B – Mixed Infrastructure

BEAD Timeline – *States*

Letters of Intent	Due July 18, 2022
Initial Planning Funds Request (Up to $1M)	Due August 15, 2022
5 Year Action Plans	han 270 days after receipt of Initial Funds request
Notification of Funding Formula Allocations	**June 2023**
Initial Proposals (20%)	**No later than 180 days after formal notification of funding formula allocations** ***Cybersecurity plans to be in place**
Final Proposals (Remaining 80%)	No later than 365 days after approval of Initial Proposal

YOU ARE HERE

Enhanced ACAM Timeline

- **August 30, 2023 -** FCC releases official E-ACAM offers to carriers
- Carriers must decide by **September 29, 2023**
- Implement & submit operational Cybersecurity and Supply Chain risk management plans to USAC by **January 1, 2024**

ARE YOU
READY
?

Where are the Cyber requirements coming from?

And

What are the requirements?

Executive Order on Improving National Cybersecurity

- Executive Order 14028, May 12, 2021:

  “It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security.”

- Effects of insecurity:
  - Financial Loss
  - Reputational Damage
  - Disclosure of Sensitive Information

MAY 12, 2021

Executive Order on Improving the Nation’s Cybersecurity

Presidential Executive Order Includes...

- Removing Barriers to Sharing Threat Information
- Modernizing Federal Government Cybersecurity
- Enhancing Software Supply Chain Security
- Establishing a Cyber Safety Review Board
- Standardizing the Federal Government’s Playbook for Responding to Cybersecurity Vulnerabilities and Incidents
- Improving Detection of Cybersecurity Vulnerabilities and Incidents
- Improving the Federal Government’s Investigative and Remediation Capabilities

Executive Order 14028 → BEAD, E-ACAM?

- Cybersecurity requirements are now conditions of federal funding
- If you provide service to an office of the Federal government, you are required to report when you discover a cyber incident involving the product or service delivered to that agency.
- If you do not provide the Federal government with service, your Plan should still reflect that you are prepared to satisfy the requirements of EO 14028 should you eventually contract with them.
- EO 14028 has an emphasis on Public and Private sector cyber communication

What Are the Next Steps?

- ISPs interested in Federal funding must get started with developing Cybersecurity Plans and Supply Chain Policies to prepare for attestation.
- Study the NIST Cyber Framework, Executive Order, and other related documents .
- Implement Plans, Policies and Playbooks to demonstrate Cybersecurity posture and diligence.

What does a Cybersecurity Plan entail?

Cybersecurity Plan for BEAD, E-ACAM

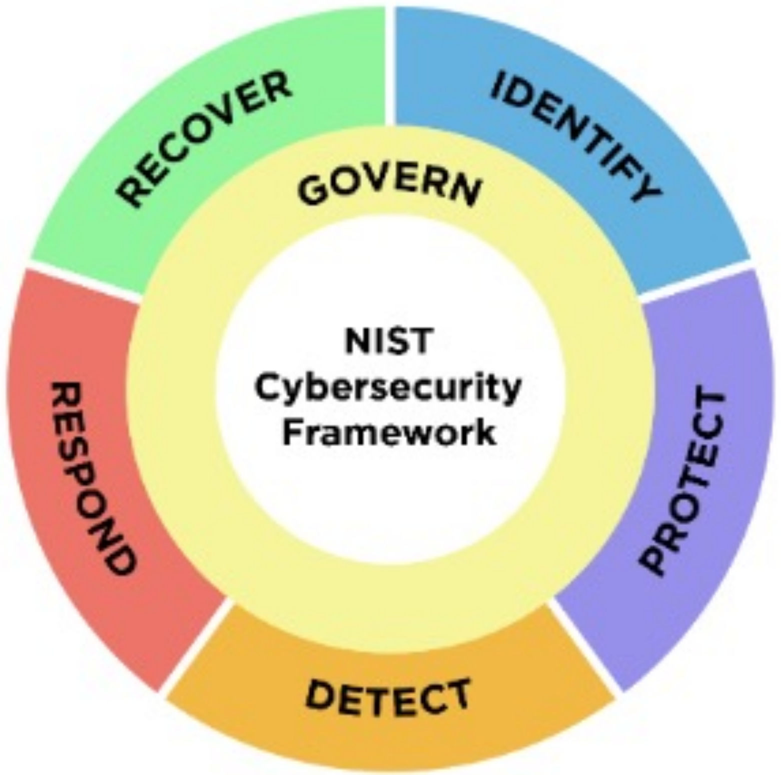
- Requirement: Have a Cybersecurity Plan in place that is either…
  - Operational (if already providing service prior to the awarding of the grant/funding)
  - Ready to be operationalized upon providing services.
- The Plan must reflect the *latest version* of the NIST Cybersecurity Framework and the standards and controls set forth in Executive Order 14028 and specify the security and privacy controls being implemented.
- Reevaluate and update the plan periodically and as events warrant.
- Submit the Plan to the State/USAC prior to the allocation of funds along with any significant changes (within 30 days of the change)

About the NIST Cybersecurity Framework

- Intended to be broad in scope and apply to all industries.
- Developed to help an organization prioritize critical cybersecurity activities and to connect organizations with resources and guidance on how to perform those activities.
- The Framework enables organizations (regardless of size)
  - To implement a degree of cybersecurity risk, or cybersecurity sophistication.
  - To apply the principles and best practices of risk management to improving security and resilience.

NIST Cybersecurity Framework

1. **Identify** – Systems, people, assets, data, and capabilities
2. **Protect** – Implement safeguards to ensure delivery of critical services
3. **Detect** – Implement systems or activities that identify the occurrence of a cyber event
4. **Respond** – Implement activities to act against detected cybersecurity incidents
5. **Recover** – Implement plans for resilience to restore capabilities or services that were impaired
6. **Govern –** Establish and monitor the organization's cyber risk management strategy, expectations, and policy



NIST Cybersecurity Framework

- The Framework is **NOT** intended to be a checklist.
- Your Plan should **REFLECT** the Framework, meaning that your Plan conveys that you are familiar with the Framework and have built your Plan with it in mind and using it as a tool.
- Familiarize your management teams with how the Cybersecurity Framework may alter business processes.
- Implement the Cybersecurity Framework and reference it in your policy documents.

What is a Supply Chain Plan?

Supply Chain Risk Management Plan

- Have a Cybersecurity Supply Chain Risk Management (C-SCRM) Plan in place that is either:
  - Operational (if already providing service prior to the awarding of the grant)
  - Ready to be operationalized upon providing services.
- The Plan must be based on key practices discussed in NIST publication NISTIR 8276 and NIST 800-161 and includes the controls being implemented.
- Reevaluate and update the plan periodically and as events warrant.
- Submit the Plan to the State/USAC prior to the allocation of funds along with any substantive changes (within 30 days of the change)

Supply Chain Threats

- Supply chain threats come from vulnerabilities originating outside your direct control.
- Examples:
  - Counterfeit products
  - Hardware or software delivered with malware or unwanted functionality
  - Vulnerabilities in third-party providers' systems and networks
  - Poor quality manufacturing or disposal practices
  - Insider Threats

NISTIR 8276: Key Practices

Key Practices

1. Integrate C-SCRM across the organization
2. Establish a formal C-SCRM program
3. Know and manage critical components and suppliers
4. Understand the organization’s supply chain
5. Closely collaborate with key suppliers
6. Include key suppliers in resilience and improvement activities
7. Assess and monitor throughout supplier relationships
8. Plan for the full lifecycle

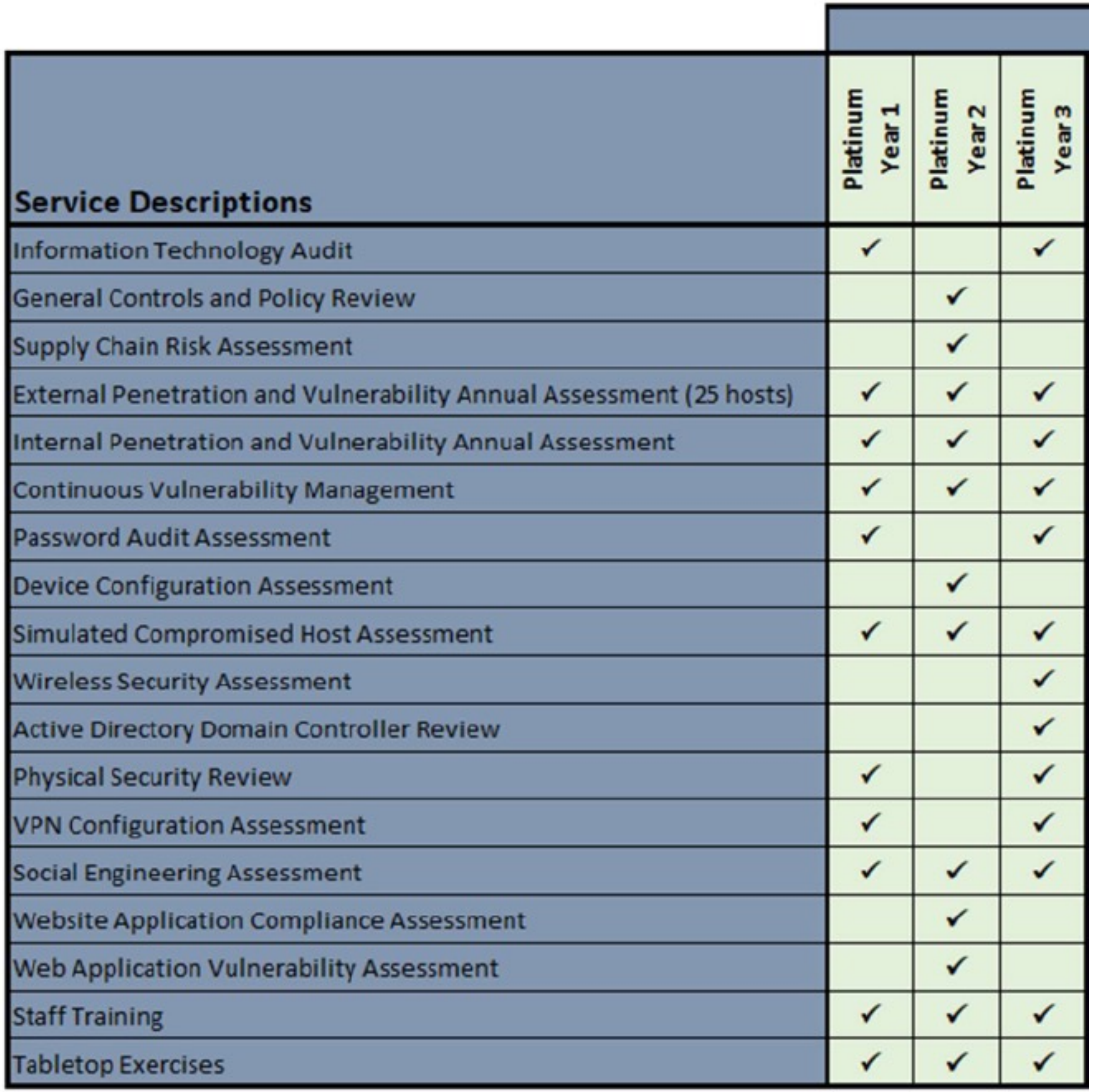
Supply Chain Resource: NIST 800-161

- Provides guidelines and best practices for managing supply chain risks
- Appendices for guidance and context
  - C-SCRM Controls
  - Risk Exposure Framework
  - C-SCRM Activities in the Risk Management Process

Three Major Parts to the Cybersecurity Requirements

1. Implement a Cybersecurity Risk Management Plan
2. Implement a Supply Chain Risk Management Plan
3. ISPs will need to follow State and USAC specific guidelines on how to attest to the satisfactory **implementation** of such plans and related requirements.

VPS Cybersecurity Playbook + Templates



Service Descriptions	Platinum Year 1	Platinum Year 2	Platinum Year 3
Information Technology Audit	✓		✓
General Controls and Policy Review		✓	
Supply Chain Risk Assessment		✓	
External Penetration and Vulnerability Annual Assessment (25 hosts)	✓	✓	✓
Internal Penetration and Vulnerability Annual Assessment	✓	✓	✓
Continuous Vulnerability Management	✓	✓	✓
Password Audit Assessment	✓		✓
Device Configuration Assessment		✓	
Simulated Compromised Host Assessment	✓	✓	✓
Wireless Security Assessment			✓
Active Directory Domain Controller Review			✓
Physical Security Review	✓		✓
VPN Configuration Assessment	✓		✓
Social Engineering Assessment	✓	✓	✓
Website Application Compliance Assessment		✓	
Web Application Vulnerability Assessment		✓	
Staff Training	✓	✓	✓
Tabletop Exercises	✓	✓	✓

Questions ?

Thank You

VantagePoint
EMPLOYEE OWNED