ZCorum™

# The Cybersecurity Policies, Plans and Practices You Must Have in Place to Qualify for BEAD, E-ACAM and Other Government Broadband Funding Programs

# Introduction

Since the global pandemic, the allocation of funds for broadband access has become a critical component of the government's agenda. Recognizing the pivotal role that robust broadband plays in fostering economic growth, policymakers have accelerated the expansion for high-speed internet to reach underserved and unserved communities through grants and funding initiatives.

The distribution of these funds to broadband providers will impact the lives of their constituents for years to come, so government leaders will look carefully at submissions from broadband providers to ensure that they have met the full requirements.

Applying for these funds is not an easy task, and now an additional layer of complexity has been added, that of cybersecurity. Governments have mandated stringent cybersecurity requirements as a prerequisite for accessing new broadband grants. This reflects a heightened awareness of the potential vulnerabilities associated with widespread connectivity and the need to safeguard critical networks from cyber threats.

For example, operators who will be providing broadband service over a network funded by BEAD or Enhanced A-CAM must have a cybersecurity plan in place that reflects the latest version of the NIST Cybersecurity Framework. And, future government funding initiatives are likely to have a cybersecurity requirement as well.

# Broadband Provider Cybersecurity Requirements You Will Have to Submit

Broadband Providers applying for funding must demonstrate that they have cybersecurity management plans that align with certain federal guidance documents.

## The Cybersecurity requirement includes four provisions:

1. The entity applying for funding must have a cybersecurity risk management plan in place that is operational or "ready to be operationalized upon providing service.
2. Improving Critical Infrastructure Cybersecurity.
3. The cybersecurity plan must be reassessed and updated regularly.
4. The plan—and any changes to it—must be submitted before grant funds will be allocated.

All four requirements must be met, but the second requirement, adhering to the NIST Framework, is where it really becomes formidable.

# National Institute of Standards and Technology Framework

NIST includes several stages you must meet to have an adequate cybersecurity plan and be eligible for funding.

- ✓ Describe their current cybersecurity posture
- ✓ Describe their target state for cybersecurity
- ✓ Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
- ✓ Assess progress toward the target state
- ✓ Communicate among internal and external stakeholders about cybersecurity risk

**NIST includes several stages you must meet to have an adequate cybersecurity plan and be eligible for funding.**

# NIST Framework Cybersecurity Plan Summary

## Core Components of NIST

**The NIST Cybersecurity Framework aids providers in establishing a cybersecurity program.**

1. **Identify**
The Identify function involves managing cybersecurity risks to systems, data, and capabilities. This includes identifying and documenting assets, business processes, roles, and responsibilities related to cybersecurity. By understanding potential vulnerabilities and the organization's risk tolerance, operators can lay the groundwork for a strong cybersecurity strategy.

2. **Protect**
The Protect function focuses on implementing safeguards to limit or contain the impact of a potential cybersecurity event. This includes having access controls, encryption, firewalls, and secure configurations in place. By implementing appropriate defenses, providers can reduce the attack openings and make it harder for threat actors to find and exploit vulnerabilities.

3. **Detect**
The Detect function involves actively monitoring systems and networks to identify cybersecurity attempts or incidents in real time. Intrusion detection systems, security event management solutions, and other monitoring tools play a key role in recognizing unauthorized activities or anomalies. Early detection allows for fast responses to mitigate potential damage.

4. **Respond**
The Respond function is about taking immediate action when a cybersecurity incident occurs. This means having defined response plans, trained personnel, and practiced procedures to handle any incidents effectively. Quick and coordinated responses can help contain the incident, minimize its impact, and restore normal operations faster.

5. **Recover**
The Recover function focuses on restoring normal operations in the event of a cybersecurity incident. This includes recovering all data, systems, and capabilities, as well as learning from the incident to improve future responses. An effective recovery process helps providers bounce back and minimize downtime, reducing the impact on operations.

# Implementing NIST Cybersecurity Framework

**By implementing these steps for each core component, providers will better protect their systems and data from threats.**

## 1 Identify:

- Understand your cybersecurity requirements, and the resources that need protection.
- Create an inventory of assets, data, systems, and personnel, and understand their roles and importance.
- Assess your risk based on vulnerabilities, and potential impacts.
- Develop a companywide understanding of cybersecurity risks and establish a risk management strategy.

## 2 Protect:

- Implement access controls to restrict unauthorized access to your systems and data.
- Ensure secure configuration of your systems, software, and all devices to reduce any potential vulnerabilities.
- Employ strong authentication methods, such as multi-factor authentication, to enhance user verification.
- Apply encryption to protect sensitive data both in idle and during transmission.
- Establish and enforce policies and procedures for secure operations across all departments in your entire organization.

## 3 Detect:

- Implement a continuous monitoring program to identify and respond to cybersecurity events in real time.
- Use intrusion detection systems such as firewalls, and other technologies to detect unauthorized activities.
- Collect and analyze logs and security information to identify potential threats or breaches.
- Develop incident detection and response action plans to minimize the impact of cybersecurity incidents.

## 4 Respond:

- Establish an incident response plan that outlines the steps to take when a cybersecurity incident occurs.
- Form an incident response team and define their roles and responsibilities.
- Communicate with your personnel and with any external partners if an incident occurs.
- Execute the incident response plans to contain the impact of the incident.
- Learn from any incidents and update your responses to improve future handling.

## 5 Recover:

- Implement strategies to restore any affected systems and data after an incident.
- Ensure backups are regularly tested and can be used to recover from incidents.
- Conduct reviews to analyze your incident responses and recovery processes.
- Update your risk management and business continuity plans based on incident reviews
- Continuously assess and adjust your recovery strategies to enhance resilience.

# It's Too Vital to Approach it Alone

The amount of information needed to follow the NIST Framework for submitting your cybersecurity plan seems overwhelming, especially since it's only one of the requirements that must be met when applying for funding. The process can be difficult and lengthy, and you want to get it right to avoid any delays.

Now is a good time to partner with us, so we can help navigate this complicated environment with you. ZCorum is ready with extensive cybersecurity experience that can help you meet the NIST Framework criterion in order to apply for funding. Don't wait. Contact us today and let's get you prepared for your submission.

# Next Steps

Cybersecurity is an ongoing process and requires constant monitoring for new threats. Protecting your network is an investment in its long-term stability and reputation. By prioritizing cybersecurity and utilizing the government grant funding, you can significantly enhance your company's resilience against cyberattacks.

Fortunately, you don't need to do all of this on your own. Let ZCorum be your cybersecurity team. In addition to expert advice on the security policies you should have in place, we offer a managed, comprehensive Cybersecurity Solution that includes intrusion detection software and a fully staffed Security Operations Center that watches over your network 24x7. We can also deploy managed Endpoint Detection and Response (EDR) to protect the endpoints on your network. You can have immediate peace of mind knowing there is a robust defense in place protecting your network and your business from the inevitable threats and attacks that will come. For more information on how we can help, be sure to **visit our website** or contact us at 800-909-9441.

ZCorum™

**4501 North Point Parkway,**
**Suite 125**
**Alpharetta, GA 30022**
**Toll Free: 1-800-909-9441**
**info@ZCorum.com**

ZCorum provides broadband Internet and communication solutions to telcos, cable companies, utilities, and municipalities, assisting in all facets of broadband implementation, integration, engineering and consulting, network monitoring and diagnostics. ZCorum also offers wholesale, privatelabeled Internet services, including data and VoIP provisioning, email, Web hosting, and 24x7 support for end-users, enabling service providers to compete effectively in their local rural and suburban markets. ZCorum is headquartered in Alpharetta, GA.

# More Resources

**More specifics for the cybersecurity requirements can be found in these government documents:**

**The Cybersecurity: NIST Framework for Improving Critical Infrastructure Cybersecurity:**
https://www.nist.gov/cyberframework

**Cybersecurity: Standards and controls set forth in U.S. Executive Order 14028:**
https://www.gsa.gov/technology/technology-products-services/it-security/executive-order-14028-improving-the-nations-cybersecurity

**Product Sheet:** Cybersecurity Solutions Made Simple

ZCorum™

**4501 North Point Parkway,**
**Suite 125**
**Alpharetta, GA 30022**
**Toll Free: 1-800-909-9441**
**info@ZCorum.com**

ZCorum provides broadband Internet and communication solutions to telcos, cable companies, utilities, and municipalities, assisting in all facets of broadband implementation, integration, engineering and consulting, network monitoring and diagnostics. ZCorum also offers wholesale, privatelabeled Internet services, including data and VoIP provisioning, email, Web hosting, and 24x7 support for end-users, enabling service providers to compete effectively in their local rural and suburban markets. ZCorum is headquartered in Alpharetta, GA.