BORDERHAWK

BEAD CYBERSECURITY & SCRM PREPARATION

BorderHawk is providing its "BorderHawk Method" to help the rural telco community understand this requirement and develop a manageable way forward.

BEAD Cybersecurity & Supply Chain Risk Management Preparation

The **Broadband Equity, Access, and Deployment (BEAD) Program**, provides $42.45 billion to expand high-speed internet access by funding planning, infrastructure deployment and adoption programs in all 50 states, Washington D.C., Puerto Rico, the U.S. Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

The BEAD grant program has been described as a once in a generation opportunity. An opportunity that see's the small to medium sized rural telco providers standing at the dividing line between the major metropolitan areas served by the large multi-regional, multi-state providers and the predominate portion of the un/underserved population. It is these rural, often family run sub-grantees that BorderHawk serves.

Protecting the small rural provider in the telecom arena creates important competition and brings local service to hard-to-reach areas that often fall outside of the large providers' business model. Many of the un/underserved communities will have no quality internet service available if the small rural provider opts out of the BEAD Grant program.

The grant requires the Implementation of an Information Risk Management program reflecting NIST CSF 1.1, Executive Order 14028, NISTIR 8276 and NIST 800-161 as identified on page 70 of the BEAD NOFO.

> BorderHawk is providing its "*BorderHawk Method*" to help the rural telco community understand this requirement and develop a manageable way forward.

Within this framework there are specific processes identified to ensure the rural broadband provider is following NIST CSF and has "a prioritized, flexible, repeatable, performance based, and cost-effective approach, including information security measures and controls adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risk."

NIST CSF processes are:

1. Prioritize and Scope
2. Orient
3. Create a Current Profile
4. Conduct a Risk Assessment
5. Create a Target Profile
6. Determine, Analyze and Prioritize the Remediation of Gaps.
7. Implement an Action Plan

Core Functions

NIST CSF is broken into 5 core functions (Identify/Protect/Detect/Respond/Recover). Across the Five functions are 23 Categories and 108 sub-categories. Each Sub-Category represents an objective that is intended to be evaluated and, where appropriate, met. NIST CSF calls out the "what", the organization is responsible for determining the how.

Within this document we will help shed some light on what the "what" means as well as describe how this process can be followed and the requirement met.

The BEAD NOFO states on page 70 (section IV. Program Structure, Sequencing and Requirements; C. Program Requirements; 2. Obligations for Subgrantees Deploying Network Projects; c. Service Obligations; vi. Cybersecurity and Supply Chain Risk Management):

With respect to cybersecurity, prior to allocating any funds to a subgrantee, an Eligible Entity shall, at a minimum, require a prospective subgrantee to attest that:

1. The prospective subgrantee has a cybersecurity risk management plan (the plan) in place that is either:

a. operational, if the prospective subgrantee is providing service prior to the award of the grant; or

b. ready to be operationalized upon providing service, if the prospective subgrantee is not yet providing service prior to the grant award;

2. The plan reflects the latest version of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (currently Version 1.1) and the standards and controls set forth in Executive Order 14028 and specifies the security and privacy controls being implemented;

3. The plan will be reevaluated and updated on a periodic basis and as events warrant; and

4. The plan will be submitted to the Eligible Entity prior to the allocation of funds. If the subgrantee makes any substantive changes to the plan, a new version will be submitted to the Eligible Entity within 30 days. The Eligible Entity must provide a subgrantee's plan to NTIA upon NTIA's request.

With respect to supply chain risk management (SCRM), prior to allocating any funds to a subgrantee, an Eligible Entity shall, at a minimum, require a prospective subgrantee to attest that:

1. The prospective subgrantee has a SCRM plan in place that is either:

a. operational, if the prospective subgrantee is already providing service at the time of the grant; or

b. ready to be operationalized, if the prospective subgrantee is not yet providing service at the time of the grant award;

2. The plan is based upon the key practices discussed in the NIST publication NISTIR 8276, Key Practices in Cyber Security Supply Chain Risk Management: Observations from Industry and related SCRM guidance from NIST, including NIST 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations and specifies the supply chain risk management control being implemented;

3. The plan will be reevaluated and updated on a periodic basis and as events warrant; and

4. The plan will be submitted to the Eligible Entity prior to the allocation of funds. If the subgrantee makes any substantive changes to the plan, a new version will be submitted to the Eligible Entity within 30 days. The Eligible Entity must provide a subgrantee's plan to NTIA upon NTIA's request.

An Eligible Entity also must ensure that, to the extent a BEAD subgrantee relies in whole or in part on network facilities owned or operated by a third party (e.g. purchases wholesale carriage on such facilities), obtain the above attestations from its network provider with respect to both cybersecurity and supply chain risk management practices.

Timeline

To meet the requirements established in the BEAD NOFO BorderHawk has planned its recommendations around industry best practices, including industry specific guidance developed for Broadband and Telecommunications. See Figure 1 and accompanying bullets below to give a brief overview and explanation of the history of cybersecurity recommendations for Telecommunications:

In February of 2014 the National Institute of Standards and Technology (NIST) released v1.0 of its Cybersecurity Framework (CSF) in response to Executive Order 13636.

In March of 2015 the Communications Security, Reliability, and Interoperability Council (CSRIC) IV Working Group 4 (WG4) created guidance on the implementation of CSF v1.0 for the Telecommunications industry.

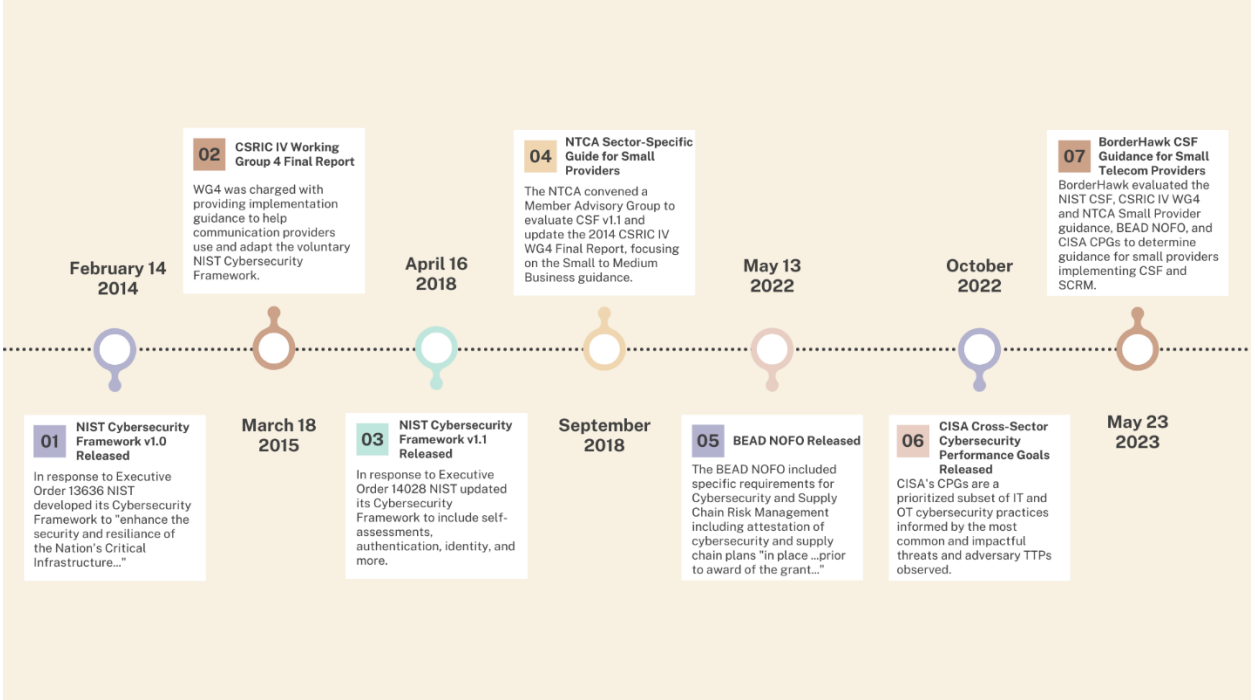
In April of 2018 NIST released v1.1 of CSF in response to Executive Order 14028.

In September of 2018 the National Telephone Cooperative Association (NTCA) convened a Member Advisory Group to evaluate CSF v1.1 and update the 2014 CSRIC IV WG4 Final Report, focusing on Small to Medium guidance.

In May of 2022 the BEAD NOFO was published including specific requirements for Cybersecurity and Supply Chain Risk Management.

In October of 2022 the Cybersecurity and Infrastructure Security Agency (CISA) released Cross-Sector Cybersecurity Performance Goals (CPGs) to prioritize a subset of IT and OT cybersecurity practices informed by the most common and impactful threats and adversary Tactics, Techniques, and Procedures (TTPs) observed.

Figure 1



We leveraged these documents in sequence to develop guidance for the Telecommunications industry to implement the requirements of Cybersecurity and Supply Chain Risk Management required by BEAD with a focus on the largest risk areas commonly affecting Critical Infrastructure.

Methodology

BorderHawk used NIST CSF 1.1, the BEAD NOFO, available guidance from WG4, NTCA and NTIA to develop a set of priorities that include Immediate, High, Medium and Low prioritizations. The Immediate prioritization step gives the subgrantee applicants a specific set of actions to initiate development of their plans with the goal of achieving them by the time of their application. Addressing the Immediate subcategories support the goal of creating the base risk management plan. This will be the foundation for future decision making and production of an actionable Plan of Actions and Milestones (PoAMs). The Immediate Phase coupled with the High Priority Phase will produce an operational cybersecurity program. This resulting program would satisfy the reflection requirement of NIST CSF 1.1, Executive Order 14028, NISTIR 8276 and NIST 800-161 and SCRM required with in the BEAD NOFO.

The BorderHawk Immediate CSF subcategories are as follows:

ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated.

ID.BE-4: Dependencies and critical functions for delivery of critical services are established.

ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.

ID.RA-1: Asset vulnerabilities are identified and documented.

ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources.

ID.RA-3: Threats, both internal and external, are identified and documented.

ID.RA-4: Potential business impacts and likelihoods, and impacts are used to determine risk.

ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.

ID.RA-6: Risk responses are identified and prioritized.

ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.

ID.RM-2: Organizational risk tolerance is determined and clearly expressed.

ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.

To meet this goal, we suggest organizations follow NIST CSF's implementation guidance for new or improving programs by walking through BorderHawk's recommended method (based on NIST CSF's 7 step process):

1. Prioritize and Scope – Determine business/mission objectives and high-level priorities and decide on a risk model and approach. (ID.BE-3, ID.BE-4)
2. Orient – Identify key assets (People, Processes, Technology, and Facilities) and identify applicable laws and regulations. (ID.GV-3)
3. Create a Current Profile – Describe the current objectives accomplished by the organization, the degree to which the objective is accomplished, and describe the specific security controls in place.
4. Establish Risk Tolerances – Those at the highest level in the organization must decide what constitutes an acceptable risk to them, what must be mitigated, and when a risk should be avoided entirely. (ID.RM-2, ID.RM-3)
5. Determine C-SCRM program readiness – Determine how many of the recommended practices for C-SCRM from NIST the organization currently meets, and what should be improved.
6. Conduct an Information Risk Assessment – Identify the organization's critical assets and determine, for each asset, vulnerabilities that may affect it, potential threat events, the

likelihood and impact of each event, and a risk of and to the asset. Include your supply chain in this assessment. (ID.RA-1, ID.RA-2, ID.RA-3, ID.RA-4, ID.RA-5, ID.RM-1)

7. Create a Target Profile – Describe the objectives needed for the organization to mitigate risks to acceptable levels based on the Risk Tolerances defined. When determining Target Profiles, the organization is encouraged to consider our determination of High, Medium, and Low Priorities.
8. Determine, Analyze, and Prioritize Gaps – Create a PoAM to cover any entries in the Target Profile which is not sufficiently covered in the Current Profile. Each entry in the PoAM should have personnel assigned for remediation and resources allocated to the project. Determination of exact plans is advised but is not strictly required. (ID.RA-6)

For the supply chain risk management plan, the BorderHawk method addresses these requirements during the review of the current and target profiles and across the High, Medium, and Low priority phases of implementation and operation.

There are two spreadsheets that correspond with this booklet (CSF Priority Comparison and the Copy I-M Combined V2). You may download these from our site or receive via email.

Contact Us

If you would like to learn more, or discuss your current situation, please reach out to BorderHawk and one of our cyber specialists will schedule a strategy session. Give us a call at 770-607-7384 or email David.Bauer@BorderHawk.com.