

Discussion Draft/Template for Cybersecurity and Supply Chain Risk Management Plan

**Disclaimer:**

This Discussion Draft/Template for Cybersecurity and Supply Chain Risk Management Plan (“Discussion Draft”) is offered to help your company begin the process of developing its own cybersecurity plan and is intended to spur discussion. Your company’s cybersecurity and supply chain risk management plan should accurately reflect your company’s efforts to offer secure and reliable service to customers. The National Telecommunications Cooperative Association d/b/a NTCA – The Rural Broadband Association (“NTCA”) is offering this Discussion Draft for general information purposes only, and nothing contained herein constitutes legal advice or opinions of any kind.  You use this document at your own risk, and you should not use it without first seeking legal and other professional advice. NTCA makes no representations or warranties, express or implied, with respect to the Discussion Draft, including without limitation any warranties of fitness for a particular purpose. NTCA and its affiliates (and any of their respective directors, officers, agents, contractors, interns, suppliers, and employees) are not responsible for, and expressly disclaim, all liability for, damages of any kind arising out of use, reference to or reliance of any information contained within the Discussion Draft or Cybersecurity Series. Although the Cybersecurity Series may include links providing direct access to internet resources, including websites, NTCA is not responsible for the accuracy or content of information contained in these sites.

Cybersecurity and Supply Chain Risk Management Plan

[NTCA Member Company Name]

[Version Number]

[Applicable Period]

[Description of intended audience and scope of authorized distribution]

Authors: [Names and Roles]

Approved by: [Name, Role]

**Table of Contents**

1. Cybersecurity and Supply Chain Risk Management Plan
   1. Mission and Objectives
   2. General Purpose and Scope
   3. Corporate Governance and Certification
   4. Plan Implementation and Updates
2. Plan Implementation
   1. Phase One: Initial and Continuous Planning and Governance Priorities
   2. Phase Two: Primary Operational Priorities
   3. Phase Three: Longer-Term Operational Priorities

1. **Cybersecurity and Supply Chain Risk Management Plan**

***Mission and Objectives:***

[Insert Company’s organizational mission statement.]

[Company’s] primary objective in implementing our Cybersecurity and Supply Chain Risk Management Plan (“Plan”) is secure, reliable [telecommunications and/or broadband] service for our customers. In striving to meet this objective, we have also designed and implemented the Plan to fulfill the requirements that apply to [Enhanced A-CAM carriers/reference to other filing requirement]

***General Purpose and Scope:***

[Company’s] comprehensive Plan derives from NIST and CISA guidance, tailored to our specific operational needs. Specifically, the Plan reflects Draft Version 2.0 of NIST’s Cybersecurity Framework (“CSF 2.0”) and implements the Draft’s new Core Function, Governance, and the new Category, Supply Chain Risk Management. Through its three-phase implementation of CSF 2.0 as described below in Part 2 (Implementation), the Plan also reflects CISA’s Cybersecurity Performance Goals (CPGs) and incorporates NIST’s guidance on supply chain risk management, namely the Key Practices identified in NISTIR 8276 and related guidance from SP 800-161.

***Corporate Governance and Certification:***

[Company’s Board and/or Executive Officers] certify review and approval of the Plan for the purposes of meeting the above objectives and for compliance with [Enhanced A-CAM] requirements and take ultimate responsibility for its implementation as outlined below.

On a day-to-day basis, pursuant to the Governance function described below, [named Company executive] oversees implementation of the Plan. [Insert additional brief description of executive roles and responsibilities as appropriate.]

***Plan Implementation and Updates:***

The Plan consists of three interrelated and mutually reinforcing phases:

* Phase One: Initial and Continuous Planning and Governance Priorities
* Phase Two: Primary Operational Priorities
* Phase Three: Longer-Term Operational Priorities

Below we describe implementation of these three phases, including reference to the relevant CSF categories and subcategories, CISA CPGs, and NIST supply chain guidance.

The Plan is purposely designed for flexibility to account for the dynamic and fluid threat environment. We regularly monitor implementation effectiveness and adapt Plan implementation, as necessary. Pursuant to FCC rules for [Enhanced A-CAM carriers], we will file an updated Plan within 30 days of any substantive modification to the Plan.

***Phase One: Initial and Continuous Planning and Governance Priorities***

The first phase of implementing the plan focuses on asset management, data management, and risk assessment. This phase is both an initial step and continuous in implementation.

Asset Management.[[1]](#footnote-1) In [month/year] we conducted our initial formal inventory of our hardware, software, services, and systems. We update inventories at least monthly for IT and OT assets. On [date], we formally established our asset classification parameters and classified our assets accordingly.

Data Management.[[2]](#footnote-2) On [date], we formally established our data classification parameters and classified our data accordingly. We map internal and external data flows according to this classification.

Risk Assessment and Management.[[3]](#footnote-3) Our basic approach to risk assessment and management focuses on threats, vulnerabilities, and risk evaluation, along with a particular focus on supply chain risk management:

* *Threats*. We have formally identified and prioritized internal and external threats to the organization. We constantly evaluate and re-evaluate threat intelligence from [CyberShare: The Small Broadband Provider ISAC and other resources].
* *Vulnerabilities*. We constantly seek to determine and address known vulnerabilities in our systems, including through checking CISA’s Known Exploited Vulnerability Catalog. We ensure that all known vulnerabilities are patched or otherwise mitigated. On [date], we formally established our patch management policy.
* *Risk Evaluation*. We seek to assess, score, and prioritize risks for purposes of Board and Executive risk management. As noted above, [the Board and/or Executive Officer] have approved the Plan, including the risk management strategies contained within it. Pursuant to their direction, we have a timeline and process for re-evaluation.
* *Supply Chain*.[[4]](#footnote-4) We have developed a formal Supply Chain Risk Management Policy that incorporates the Key Practices of NISTIR 8276 and related guidance in NIST SP 800-161. We prioritize our suppliers by criticality, and we have a risk-informed “allow list.” We pre-assess all of our suppliers and address identified risks through Service-Level Agreements. We require notice of cybersecurity incidents affecting our suppliers, and we require identification of known vulnerabilities by our suppliers. We regularly reassess all suppliers.

***Phase Two: Primary Operational Priorities***

The second phase of our Plan pertains to ongoing operational priorities, including network segmentation, identity and access management, data protection, activity logging, device usage, change management, training, and incident response.

Network Segmentation.[[5]](#footnote-5) Our policy for network segmentation prioritizes resources to secure IT/OT interfaces. Necessary connections between OT and IT networks are protected via [describe high-level configuration]. No OT assets are exposed to the internet unless it is necessary for operations, and in those cases, we employ exceptional additional protections. Likewise, we limit the exposure of services, such as remote desktop protocol, to the public internet, and have put in place compensating controls for those services which are exposed.

Identity and Access Management.[[6]](#footnote-6) Our policies for identity and access management include password rules that require password length of [insert] characters, as well as regular password changes. We also employ account lockout policies that [describe high-level attributes]. Our authentication procedures maximize the principles of “least privileged” and “zero trust,” and we [employ] [are implementing] multi-factor authentication. Our remote access policies employ these practices as well. Our offboarding process ensures that logical and physical access is terminated for departing employees on the day of their departure. We audit and assess these processes to ensure their effectiveness.

Data Protection.[[7]](#footnote-7) We protect data at rest and in-motion. Our encryption policies ensure that no sensitive data is stored in plaintext, and that other data at-rest and data in-transit (including e-mail) is encrypted, when technically feasible. We also protect passwords via [password keeper or other safekeeping]. We back up our data at least once per year and test backups annually. Critical information about OT systems is backed-up (configurations, roles, programmable controller logic, engineering drawings and tools). Further, we review and amend our encryption practices to address known degradations.

Change Management.[[8]](#footnote-8) Our change management policy has established baseline configurations for critical IT and OT systems (including roles, programmable controller logic, engineering drawings and tools) and network topology. Periodic reviews and updates are performed and tracked on a recurring basis.

Logging, Monitoring, and Threat Detection.[[9]](#footnote-9) Logging and monitoring for potentially adverse events is an ongoing function, which is mapped to known threats to the organization. We collect and monitor activity logs from all available sources, including IT and OT infrastructure. Physical access to sensitive systems is also monitored. Further, external service provider activities and services are monitored, where feasible. Logs are stored securely for [insert time period] in [identify any system(s), such as intrusion detection systems that actively monitor]. Automated notifications of anomalies and alerts to the absence of log data are enabled.

Device Usage.[[10]](#footnote-10) Our policy for device usage prohibits connection of unauthorized devices and also disables device connections where feasible, with exception procedures where not feasible. Installation and execution of unauthorized software are prevented. We disable macros and other embedded code by default and apply an exception policy if necessary. Personnel activity and technology usage are monitored to find potentially adverse events.

Training.[[11]](#footnote-11) The Plan requires annual cybersecurity training for all employees, and specialized annual training for all privileged users and personnel focused on OT-specific threats.

Incident Response.[[12]](#footnote-12) We have developed, implemented, and exercised a Cyber Incident Response Plan (CIRP) that is understood by all relevant employees within the organization. The CIRP includes policies for information-sharing during an incident, including regulatory incident-notification requirements.

Resilience and Recovery.[[13]](#footnote-13) We employ technical and policy measures to achieve organizational resilience requirements and to recover from adverse events, including [describe high-level attributes].

***Phase Three: Longer-Term Operational Priorities***

The third phase of our Plan ensures long-term risk management regarding operational priorities that will remain in place regardless of day-to-day circumstances. For example, testing and exercising our CIRP will always be a priority, so we do so [at least annually] [if more frequently, specify]. Where feasible, we include relevant suppliers in incident planning, response, and recovery activities. Similarly, we regularly conduct [internal/third-party] audits of our cybersecurity and supply chain security risk management posture, as well as penetration tests to evaluate operational capabilities. The CIRP is updated within a risk-informed timeframe based on internal and external developments.[[14]](#footnote-14)

Likewise, our [General Counsel or other executive] has established processes to monitor and manage all legal, regulatory, and contractual requirements that pertain to this Plan, and our [hiring manager or other executive] has built cybersecurity and supply chain security into our hiring, training, and retention processes.[[15]](#footnote-15)

For our equipment, systems, and data, we employ lifecycle management, including monitoring our supply chains, replacing equipment that poses undue risks, and implementing data retention and destruction policies.[[16]](#footnote-16)

Collectively, these steps inform our efforts to continually review and improve our Plan and its various risk management components.[[17]](#footnote-17)

**CERTIFICATION**

I, [executive], hereby certify that the above-described Plan has been adopted by [Company] and, to the best of my knowledge, information, and belief, is being implemented accordingly.

[signature block]

1. *NISTIR 8276 Key Practices* and related guidance in *NIST SP 800-161*. *CSF subcategories* ID.AM-01; ID.AM-02; ID.AM-04; ID.AM-05. *CISA CPG* 1.A. [↑](#footnote-ref-1)
2. *CSF subcategories* ID.AM-03; ID.AM-07. [↑](#footnote-ref-2)
3. *NISTIR 8276 Key Practices* and related guidance in *NIST SP 800-161*. *CSF subcategories* GV.OC-01; GV.OC-02; GV.OC-04; GV.OC-05; GV.RR-01; GV.RR-02; ID.RA-01; ID.RA-02; ID.RA-03; ID.RA-04; ID.RA-05; ID.RA-06; ID.RA-8; GV.RM-01; GV.RM-02; GV.RM-03; GV.RM-04; GV.RM-05; GV.RM-06; GV.RR-03; GV.PO-01. *CISA CPGs* 1.B; 1.C; 1.D; 1.E; 4.B; 4.C. [↑](#footnote-ref-3)
4. *NISTIR 8276 Key Practices* and related guidance in *NIST SP 800-161*. *CSF subcategories* ID.RA-09; GV.SC-01; GV.SC-02; GV.SC-03; GV.SC-04; GV.SC-05; GV.SC-06. *CISA CPGs* 1.G; 1.H; 1.I; 2.Q. [↑](#footnote-ref-4)
5. *CSF subcategory* PR.IR-01. *CISA CPGs* 2.F; 2.W; 2.X. [↑](#footnote-ref-5)
6. *CSF subcategories* PR.AA-01; PR.AA-02; PR.AA-03; PR.AA-04; PR.AA-05; PR.AA-06. *CISA CPGs* 2.A; 2.B; 2.C; 2.D; 2.E; 2.G; 2.H; 2.V. [↑](#footnote-ref-6)
7. *CSF subcategories* PR.DS-01; PR.DS-02; PR.DS-10; PR.DS-11. *CISA CPGs* 2.K; 2.L; 2.M; 2.R. [↑](#footnote-ref-7)
8. *NISTIR 8276 Key Practices* and related guidance in *NIST SP 800-161*. *CSF subcategories* ID.RA-07; PR.PS-01; DE.CM-09. *CISA CPGs* 2.O; 2.P. [↑](#footnote-ref-8)
9. *CSF subcategories* PR.PS-04; DE.CM-01; DE.CM-02; DE.CM-06; DE.AE-02; DE.AE-03; DE.AE-04; DE.AE-06; DE.AE-07. CISA CPGs 2.T; 2.U; 3.A. [↑](#footnote-ref-9)
10. *CSF subcategories* PR.PS-05; DE.CM-03. *CISA CPG* 2.N. [↑](#footnote-ref-10)
11. *CSF subcategories* PR.AT-01; PR.AT-02. *CISA CPGs* 2.I; 2.J. [↑](#footnote-ref-11)
12. *CSF subcategories* DE.AE-08; RS.MA-01; RS.MA-02; RS.MA-03; RS.MA-04; RS.MA-05; RS.AN-03; RS.AN-06; RS.AN-07; RS.AN-08; RS.CO-02; RS.CO-03; RS.MI-01; RS.MI-02. *CISA CPG* 4.A. [↑](#footnote-ref-12)
13. *NISTIR 8276 Key Practices* and related guidance in *NIST SP 800-161*. *CSF subcategories* PR.IR-02; PR.IR-03; PR.IR-04; RS.RP-01; RC.RP-02; RC.RP-03; RC.RP-04; RC.RP-05; RC.RP-06; RC.CO-03; RC.CO-04. *CISA CPG* 5.A. [↑](#footnote-ref-13)
14. *NISTIR 8276 Key Practices* and related guidance in *NIST SP 800-161*. *CSF subcategories* GV.SC-08; ID.IM-01; ID.IM-02; ID.IM-03; ID.IM-04. *CISA CPGs* 1.F; 2.S. [↑](#footnote-ref-14)
15. *NISTIR 8276 Key Practices* and related guidance in *NIST SP 800-161*. *CSF subcategories* GV.OC-03; GV.SC-09; GV.RR-04. [↑](#footnote-ref-15)
16. *NISTIR 8276 Key Practices* and related guidance in *NIST SP 800-161*. *CSF subcategories* GV.SC-07; GV.SC-10; ID.AM-08; PR.DS-09; PR.PS-02; PR.PS-03; PR.PS-06. [↑](#footnote-ref-16)
17. *NISTIR 8276 Key Practices* and related guidance in *NIST SP 800-161*. *CSF subcategories* GV.RM-07; GV.PO-02; GV.OV-01; GV.OV-02; GV.OV-03 [↑](#footnote-ref-17)