Pioneer Telephone Cooperative
Cyber Supply Chain Risk Management (C-SCRM) Process

Version: 1.6 | Date: July 14, 2026

Table of Contents

Document Control

Owner: Chief Information Security Officer (CISO)

Approved by: Board of Directors and General Manager

1. Purpose and Scope

This C-SCRM Plan governs how Pioneer Telephone Cooperative identifies, assesses, mitigates, and monitors supply-chain risks across planning, acquisition, deployment, operations, and end-of-life. It applies to IT/OT hardware, software, cloud and managed services, and third-party providers engaged in any project and broader operations.

2. Authority, Documentation, Monitoring, and Audit

Pioneer Telephone Cooperative has established governance, accountability, and oversight structure for the organization's Cyber Supply Chain Risk Management (C-SCRM) Program. Its purpose is to ensure that supply chain risk management activities are conducted in a consistent, documented, and auditable manner and are aligned with recognized industry standards, regulatory requirements, and organizational policies.

The section defines the frameworks that guide the program, identifies the records that must be maintained to demonstrate compliance and due diligence, and establishes requirements for monitoring, auditing, reporting, and continuous improvement. It also ensures that supply chain risk management decisions are supported by appropriate documentation, that activities can be independently reviewed and verified, and that management maintains visibility into the effectiveness of the program.

2a. Standards and Framework Alignment

Pioneer Telephone Cooperative's Cyber Supply Chain Risk Management (C-SCRM) Program is aligned with applicable industry standards and guidance, including:

- Pioneer Cybersecurity Governance & Policy v1.1
- NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for systems and Organizations
- NISTIR 8276, Key Practices in Cyber Supply Chain Risk Management
- NIST Cybersecurity Framework (CSF) 2.0
- NIST SP 800-53 security and privacy controls, where applicable

Other regulatory, contractual, and industry requirements applicable to telecommunications and broadband operations.

2b. Documentation Requirements

The organization shall maintain documentation supporting supply chain risk management activities, including:

- Supplier risk assessments and due diligence reviews
- Vendor security questionnaires and responses
- Contractual security requirements and attestations
- SBOM and HBOM records
- Exception requests and risk acceptance decisions
- Supplier monitoring results

• Audit findings and corrective action plans

• Incident reports involving third-party suppliers

• Supplier performance and risk scorecard records

Documentation shall be retained in accordance with corporate record retention requirements and be available for management review and audit purposes.

2c. Monitoring and Audit Trails

C-SCRM activities shall be documented and monitored through established business processes and systems. Audit trails shall be maintained for material supply chain risk management activities, including:

• Supplier onboarding and approval decisions

• Security review and assessment results

• Risk treatment and acceptance decisions

• Contract approval and renewal activities

• Supplier security incidents and remediation efforts

• Changes to critical supplier relationships

• Updates to supplier risk ratings

Where technically feasible, systems supporting procurement, vendor management, cybersecurity monitoring, and asset management shall maintain logs sufficient to support investigations, audits, and compliance reviews.

2d. Internal Review and Audit

The C-SCRM program shall be reviewed periodically to verify compliance with organizational policies and applicable frameworks. Reviews may include:

• Annual C-SCRM program assessments

• Periodic supplier compliance reviews

• Internal audits of procurement and vendor management activities

• Verification of supplier attestations and contractual obligations

• Review of remediation activities associated with identified deficiencies

Findings shall be documented and tracked through completion.

2e. Metrics and Reporting

Management shall periodically review supply chain risk metrics, which may include:

• Number of critical suppliers assessed

• Percentage of suppliers meeting security requirements

• Open supplier-related security findings

• Supplier incident notifications received

• Remediation performance against established timelines

• SBOM/HBOM collection and review status

Results shall be reported to executive leadership and, where appropriate, the Board of Directors.

2f. Document Control and Version Management

This C-SCRM Plan shall be maintained under the organization's document control process. Document control requirements include:

• Unique document identification

• Version numbering and revision history

• Document owner designation

• Management approval of material changes

• Scheduled review at least annually or upon significant regulatory, operational, or threat environment changes

• Retention of prior approved versions for audit and compliance purposes

All updates shall be recorded in a revision log documenting the date, nature of the change, author, reviewer, and approval authority.

3. Governance, Roles, and Responsibilities

Pioneer Telephone Cooperative maintains a formal Cyber Supply Chain Risk Management (C-SCRM) Program to identify, assess, mitigate, monitor, and report risks arising from suppliers, service providers, software vendors, hardware manufacturers, contractors, and other third parties that support the organization's business and operational objectives.

The C-SCRM Program is established to protect the confidentiality, integrity, availability, and resilience of organizational systems, networks, services, and information assets from supply chain-related threats and vulnerabilities.

C-SCRM follows the governance model defined in the Cybersecurity Governance & Policy: Board oversight → GM accountability → CISO program ownership → Directors/Managers execution (Operations, Engineering, Construction, Purchasing, Sales & Marketing, HR).

Role	Key C-SCRM Responsibilities	Accountability / Reports To
Board of Directors	Approves risk appetite; receives quarterly SCRM posture and material exceptions	N/A
General Manager (GM)	Executive accountability; resources the program; approves high-risk exceptions and major supplier decisions	Board of Directors
Chief Information Security Officer (CISO)	Owns C-SCRM; defines supplier tiering; approves due diligence; integrates with ERM; reports metrics	GM
Director of Operations	Operational controls; asset/config mgmt; acceptance testing and chain of custody	GM
Purchasing Agent	Due diligence, contract clauses, FCC Covered List checks; maintains APL	Director of Operations
Engineering / Network Manager	Technical requirements; SBOM validation; secure configurations and firmware validation	Director of Operations
Legal/Compliance	Contract security language, right-to-audit, incident notification SLAs, regulatory alignment	GM
Vendors / Contractors	Provide attestations, SBOMs, timely patches and	Contractual

	incident notifications; sub-supplier oversight	

3a. C-SCRM Program Overview

Pioneer Telephone Cooperative maintains a formal Cyber Supply Chain Risk Management (C-SCRM) Program to identify, assess, mitigate, and monitor supply chain risks across the organization.

The C-SCRM Program is governed through the organizational structure defined in Section 3, with:

• Board of Directors providing oversight

• General Manager accountable for program execution

• Chief Information Security Officer (CISO) responsible for program ownership and implementation

The program is supported by the following policies and standards:

• Pioneer Cybersecurity Governance & Policy

• Vendor and Supply Chain Risk Management controls defined in this plan

• Applicable federal and state regulatory requirements, including BEAD and NTIA guidance

Program implementation is carried out through the processes, controls, and monitoring activities defined throughout this plan.

This program ensures clear accountability, repeatable processes, and continuous oversight of supply chain risks in alignment with NIST SP 800-161r1 and NISTIR 8276.

4. Supply Chain Risk Landscape

Pioneer Telephone Cooperative recognizes that supply chain risks extend beyond cybersecurity and may affect the organization's ability to provide reliable telecommunications and broadband services. Supply chain risks shall be identified, assessed, documented, monitored, and managed throughout the supplier relationship lifecycle. The organization shall consider the following categories of supply chain risk when evaluating suppliers, products, services, and procurement decisions:

4a. Cybersecurity and Product Integrity Risks

• Compromised software, firmware, or hardware components

• Counterfeit, malicious, or tampered products

• Vulnerabilities in third-party software or open-source dependencies

• Insecure development, manufacturing, or distribution processes

• Unauthorized supplier access to systems or data

• Supply chain attacks targeting vendors or service providers

4b. Operational Risks

• Supplier service disruptions

• Manufacturing interruptions

• Labor shortages or workforce disruptions

• Transportation and logistics failures

• Supplier dependency and single-source supplier risk

• Failure of critical subcontractors

4c. Material Availability and Lead-Time Risks

• Limited availability of fiber optic cable, electronics, network equipment, and other critical materials

• Extended equipment manufacturing lead times

• Delays in obtaining replacement parts

• Supply shortages caused by demand fluctuations, disasters, or market conditions

4d. Domestic Sourcing and Regulatory Risks

• Availability of domestically produced products that satisfy applicable Buy America, Build America (BABA) requirements

• Supplier compliance with federal, state, and contractual sourcing requirements

• Regulatory restrictions affecting imports, exports, or supplier operations

• Foreign ownership, control, or influence (FOCI) concerns

4e. Financial Risks

• Supplier insolvency or bankruptcy

• Financial instability affecting supplier performance

• Mergers, acquisitions, or ownership changes

• Inability of suppliers to sustain long-term support obligations

4f. Market and Economic Risks

• Price volatility affecting equipment, software, and services

• Inflationary impacts on procurement and construction projects

• Currency fluctuations affecting international suppliers

• Changes in market demand affecting supplier capacity

4g. Geographic and Geopolitical Risks

• Political instability affecting supplier operations

• Trade disputes, sanctions, or export restrictions

• Regional conflicts affecting manufacturing or transportation

• Concentration of manufacturing in specific geographic regions

4h. Storage, Distribution, and Transportation Risks

• Damage to equipment during transportation or storage

• Theft, loss, or diversion of products

• Breakdowns in chain-of-custody controls

• Environmental conditions affecting product integrity during shipment or storage

4i. Environmental and Natural Hazard Risks

• Wildfires, floods, earthquakes, severe weather, or other disasters affecting suppliers or transportation routes

• Utility outages impacting supplier operations

• Climate-related disruptions affecting production or logistics networks

4j. Compliance and Legal Risks

• Failure to meet contractual security requirements

• Failure to maintain required certifications or attestations

• Regulatory noncompliance affecting supplier operations

• Privacy, data protection, or telecommunications compliance violations

4k. Risk Assessment and Monitoring

Supply chain risks shall be evaluated during procurement, supplier onboarding, periodic reassessments, contract renewals, and significant operational changes. Risk assessments will consider both the likelihood and potential business impact of supply chain disruptions

and will be incorporated into supplier risk ratings and sourcing decisions. Where appropriate, mitigation strategies may include:

• Maintaining alternate suppliers

• Diversifying sourcing options

• Maintaining strategic inventories of critical materials

• Contractual security and performance requirements

• Enhanced monitoring of high-risk suppliers

• Business continuity and contingency planning

• Supplier performance and risk reviews

5. Risk Appetite (C-SCRM Context)

The Risk Appetite (C-SCRM Context) section defines the level of supply chain risk Pioneer Telephone Cooperative is willing to accept in support of its business objectives. It provides guidance for management, procurement personnel, and technical staff when making decisions regarding suppliers, products, services, and risk mitigation activities.

By establishing clear risk tolerance thresholds for service availability, data protection, system integrity, and regulatory compliance, Pioneer ensures that supply chain decisions align with the organization's operational priorities, cybersecurity objectives, and commitment to providing reliable telecommunications and broadband services. This risk appetite statement also helps determine when risks must be mitigated, escalated, or formally accepted by management, ensuring consistent and accountable decision-making across the organization. Considerations include:

• Availability: No appetite for cyber-caused service outages—especially broadband, transport, and voice/E911—within a reasonable and fiscally responsible budget.

• Confidentiality: Zero tolerance for unauthorized disclosure of CPNI/PII or regulated data by suppliers or sub-suppliers.

• Integrity: Very low tolerance for unvalidated changes or unsigned updates to production systems and devices.

• Compliance: Very low tolerance for non-compliance with legal, regulatory, and grant requirements; exceptions require formal approval and remediation timelines.

6. Risk Management Framework & Process

The Risk Management Framework & Process establishes Pioneer Telephone Cooperative's structured approach for identifying, assessing, responding to, and monitoring supply chain risks throughout the lifecycle of supplier relationships. The objective is to ensure that products, services, and suppliers supporting the organization do not introduce unacceptable operational, cybersecurity, financial, regulatory, or supply chain risks.

This framework provides a consistent methodology for evaluating suppliers and products, assigning risk levels, implementing appropriate mitigation measures, and continuously monitoring for changes that could affect the security, reliability, or availability of critical services. By applying a formal risk management process, Pioneer can make informed procurement decisions, maintain compliance with regulatory requirements, strengthen supply chain resilience, and reduce the likelihood and impact of supplier-related disruptions or cybersecurity incidents. The framework includes:

• Frame: Define supplier tiers, prohibited sources, risk criteria, acceptance thresholds, reassessment cadence.

• Identify: Maintain product BOM/SBOM; map sub-tier dependencies; track legal/regulatory constraints (e.g., FCC Covered List).

• Assess: Score inherent risk by product/service; evaluate supplier security (questionnaires, certifications, attestations); validate samples and provenance.

• Respond: Mitigate via alternate sourcing, compensating controls, contract terms; or disqualify suppliers that cannot meet requirements.

• Monitor: Continuously monitor advisories/CVEs, performance, financial health, sanctions, and incident notifications; trigger re-assessment on events.

7. Secure Procurement and Continuous Supplier Monitoring

7a. Cybersecurity Integration into Procurement

Cybersecurity risk management shall be incorporated into all stages of the procurement and vendor management process for products and services that may affect organizational systems, networks, data, or operations. The procedure includes:

• Prior to contract award, the organization shall evaluate supplier cybersecurity risks using a risk-based approach that considers:

• Security program maturity and governance practices

• Compliance with applicable cybersecurity frameworks and standards

• Supply chain security controls

• Software and hardware integrity controls

• Vulnerability management practices

• Incident response capabilities

• Data protection and privacy controls

• Foreign ownership, control, or influence (FOCI) considerations where applicable

• Financial stability and operational resilience

Risk assessments shall be completed before onboarding critical suppliers, renewing contracts with critical suppliers, or acquiring products and services that support essential business functions.

7b. Supplier Risk Classification

Contracts with suppliers supporting critical functions shall include appropriate cybersecurity and supply chain risk management requirements, including security obligations, incident reporting requirements, audit rights, and applicable SBOM/HBOM provisions.

Risk assessments shall be completed before onboarding critical suppliers, renewing contracts with critical suppliers, or acquiring products and services that support essential business functions. Supplier and Product Tiering helps Pioneer Telephone Cooperative prioritize supply chain risk management efforts by categorizing suppliers, contractors, and service providers according to the potential impact their products or services could have on business operations, network reliability, cybersecurity, regulatory compliance, and customer service.

This tiered approach ensures that resources are applied where risk is greatest. Critical suppliers that support core telecommunications, broadband, cybersecurity, financial, or operational functions receive enhanced due diligence, contractual requirements, monitoring, and periodic reassessment. Suppliers with lower operational or security impact receive oversight proportional to their risk level.

By classifying suppliers into Tier 1, Tier 2, Tier 3, and Tier 4 categories, Pioneer can focus risk management activities on those relationships that are most essential to maintaining secure, reliable, and resilient services while ensuring appropriate governance across the entire supply chain. A Supplier Risk Register is maintained in the Pioneer BSS system and is updated as part of Pioneer's ongoing supply chain risk management processes.

• Tier 1 (Critical): Suppliers whose products or services are essential to core business operations, network infrastructure, cybersecurity functions, or regulatory compliance. A disruption, compromise, or failure of these suppliers could result in significant operational impact, service outages, regulatory violations, or material risk to the confidentiality, integrity, or availability of systems and data. These suppliers are subject to the highest level

of due diligence, contractual requirements, continuous monitoring, and frequent reassessment.

• Tier 2 (High): Suppliers that support important business functions, systems, or services but are not considered critical to immediate operational continuity. These suppliers may process sensitive data, provide important infrastructure or services, or have privileged or controlled access to organizational systems. A compromise or disruption could result in moderate operational, security, or compliance impacts. These suppliers are subject to enhanced due diligence, defined contractual controls, and periodic monitoring.

• Tier 3 (Moderate): Suppliers that provide products or services with limited operational or security impact. These suppliers typically do not have access to sensitive systems or data and do not directly support critical infrastructure or essential business functions. Disruption or compromise would result in minimal operational or security impact. These suppliers are subject to standard due diligence and periodic review.

• Tier 4 (Low): Suppliers that provide low-risk, non-critical products or services with no access to organizational systems, sensitive data, or network infrastructure. These suppliers have minimal impact on operations, cybersecurity, or compliance. Due diligence and oversight activities are limited and commensurate with the low level of risk.

Risk tier classification directly informs supplier monitoring frequency, contractual requirements, and reassessment intervals defined in this plan.

7c. Continuous Supplier Monitoring

The organization shall maintain an ongoing supplier monitoring program to identify changes in supplier risk throughout the supplier relationship lifecycle. Monitoring activities may include:

• Review of security incidents affecting suppliers

• Monitoring of publicly disclosed vulnerabilities and breaches

• Assessment of supplier financial condition and business viability

• Monitoring ownership changes, mergers, acquisitions, or organizational restructuring

• Review of sanctions, regulatory actions, or adverse media reports

• Evaluation of geopolitical risks affecting supplier operations or manufacturing locations

• Review of supplier security attestations and certifications

• Verification of contractual compliance with cybersecurity requirements

7d. Periodic Supplier Reassessments

Critical and high-risk suppliers shall be reassessed periodically using a risk-based frequency. Reassessments may include:

- Updated security questionnaires
- Review of SOC reports, ISO certifications, or independent assessments
- Review of vulnerability management performance
- Assessment of incident response effectiveness
- Review of business continuity and disaster recovery capabilities
- Validation of SBOM/HBOM, and component provenance information

Results shall be documented and used to update supplier risk ratings.

7e. Risk Escalation and Remediation

Where monitoring identifies increased supplier risk, management shall determine appropriate actions, which may include:

- Requiring corrective action plans
- Increasing oversight or monitoring frequency
- Limiting supplier access to systems or information
- Suspending procurement activities
- Identifying alternate suppliers
- Terminating supplier relationships where risks cannot be adequately mitigated

7f. Supplier Lifecycle Oversight

Supply chain risk management activities shall occur throughout the supplier relationship lifecycle, including:

- Planning and Acquisition
- Onboarding
- Operations and Monitoring
- Contract Renewal
- Termination and Offboarding

8. Prohibited and Restricted Sources

Pioneer Telephone Cooperative shall not procure, lease, or maintain equipment/services on the FCC Covered List or otherwise prohibited by law. Procurement has verified status and quarterly thereafter. No exceptions are permitted.

9. Supplier Security Requirements and Compliance Enforcement

Pioneer Telephone Cooperative establishes the minimum cybersecurity and supply chain security requirements that suppliers must meet to do business with Pioneer Telephone Cooperative. Its purpose is to ensure that third parties supporting the organization's operations maintain security practices that protect the confidentiality, integrity, availability, and resilience of critical systems, services, and information.

The section defines baseline security expectations, incorporates those requirements into legally binding contracts and service agreements, and establishes processes for validating supplier compliance throughout the supplier relationship lifecycle. It also outlines corrective actions and enforcement mechanisms that may be used when suppliers fail to meet established security requirements, ensuring accountability and consistent application of the organization's cybersecurity standards.

By defining clear security requirements, contractual obligations, compliance verification activities, and exception management processes, Pioneer reduces supply chain risk, strengthens third-party accountability, supports regulatory and grant compliance obligations, and helps ensure that suppliers maintain security controls consistent with the organization's risk tolerance and operational needs.

9a. Minimum Supplier Security Requirements

Suppliers that provide products, services, software, hardware, cloud services, managed services, or other solutions supporting Pioneer Telephone Cooperative operations shall comply with applicable cybersecurity and supply chain security requirements. At a minimum, suppliers shall:

• Maintain an information security program appropriate to the nature, scope, and sensitivity of the services provided.

• Implement security controls aligned with recognized industry frameworks, such as NIST Cybersecurity Framework (CSF), NIST SP 800-161 Rev. 1, NIST SP 800-53, ISO 27001, or equivalent standards.

• Maintain processes for vulnerability identification, remediation, and disclosure.

• Protect organizational data through encryption, access controls, logging, and least privilege principles.

• Implement multi-factor authentication (MFA) for privileged access and remote administrative access.

• Maintain incident response procedures and notify Pioneer of security incidents affecting organizational systems, services, or data within contractual timeframes.

• Maintain business continuity and disaster recovery capabilities appropriate to the services provided.

• Provide SBOM/HBOM, provenance attestations, and other supply-chain documentation as contractually required.

• Ensure subcontractors supporting contracted services comply with equivalent security requirements.

9b. Contractual Security Requirements

Cybersecurity and supply chain security requirements shall be incorporated into contracts, statements of work, service agreements, purchase agreements, or other binding procurement documents for applicable suppliers. Contractual requirements may include:

• Security control obligations

• Incident notification requirements

• Vulnerability management and patching obligations

• Data protection and confidentiality requirements

• Regulatory compliance obligations

• Audit and assessment rights

• Supply chain transparency requirements

• Business continuity requirements

• SBOM and HBOM delivery requirements

• Component provenance and integrity attestations

See Appendix A for contractual requirements

9c. Service-Level Agreements (SLAs)

Contracts with critical and high-risk suppliers shall establish service-level expectations supporting cybersecurity and operational resilience, including:

• Incident notification timelines

• Vulnerability remediation timelines

• Security issue response requirements

• Availability and continuity commitments

• Reporting requirements

• Corrective action expectations

These requirements shall be consistent with the organization's cybersecurity policies, risk tolerance, and operational requirements.

9d. Compliance Verification

Supplier compliance with contractual security requirements shall be verified using a risk-based approach that may include:

• Security questionnaires

• Supplier attestations

• Independent audit reports (e.g., SOC 2)

• ISO 27001 certifications

• Third-party assessments

• Review of security documentation and policies

• Review of vulnerability management performance

• Periodic compliance reviews

• On-site assessments for critical suppliers, when appropriate

Verification activities shall be documented and retained for audit purposes.

9e. Enforcement and Corrective Actions

Failure to comply with established cybersecurity or supply chain requirements may result in one or more of the following actions:

• Requests for corrective action plans

• Increased monitoring or reporting requirements

• Restrictions on system or data access

• Delayed contract renewal or procurement activities

• Suspension of new work

• Contract termination when risks cannot be adequately mitigated

Management shall document risk treatment decisions, remediation activities, and any accepted exceptions.

9f. Exception Management

Requests for exceptions to supplier security requirements shall:

• Be documented and approved by General Mamager.

• Include a risk assessment and compensating controls, where applicable.

• Specify an expiration date and review schedule.

• Be reviewed periodically to determine whether the exception remains justified.

10. Secure Procurement and Continuous Supplier Monitoring

Pioneer Telephone Cooperative integrates cybersecurity and supply chain risk management requirements directly into the Cooperative's procurement and vendor management processes. Its purpose is to ensure that supply chain risks are evaluated and addressed consistently from the earliest stages of supplier selection through procurement, deployment, ongoing operations, and contract renewal.

The workflow establishes defined checkpoints for security reviews, supplier due diligence, risk assessments, contractual protections, product validation, asset tracking, and continuous monitoring. By embedding these controls into the procurement lifecycle, Pioneer ensures that cybersecurity, regulatory compliance, product integrity, and supply chain resilience are considered before products and services are acquired, implemented, or renewed.

This process promotes accountability among procurement, engineering, operations, and cybersecurity personnel while providing documented evidence that supplier risks are identified, assessed, mitigated, and monitored throughout the supplier relationship lifecycle. The result is a more secure, compliant, and resilient supply chain that supports the reliable delivery of telecommunications and broadband services. The process includes:

• Sourcing & Requirements: Define security and compliance requirements with Engineering/CISO based on tier and risk appetite.

• RFP/RFQ Package: Include Vendor Due Diligence Questionnaire, Security Addendum, and SBOM/VEX expectations.

• Pre-Award Due Diligence: Run questionnaire; collect attestations (SOC2/ISO); perform FCC Covered List check and save snapshot with the PO record.

• Risk Assessment & Tiering: Score inherent risk, determine supplier tier, document controls and residual risk in the Register.

• Contracting: Execute Security Addendum; include right-to-audit, incident notice SLA (24–48h), SBOM obligations, MFA/logging, data protection.

• PO Issuance: Verify APL and Covered List again; attach verification to PO; set reassessment date per tier. PO will include Vendor compliance statement.

• Receiving & Acceptance: Enforce chain of custody; verify signed firmware; apply golden configs before production.

• Asset & SBOM Linkage: Record asset with firmware version and link to SBOM; enable telemetry to SIEM.

• Ongoing Monitoring: Track advisories/CVEs, performance, sanctions; require timely patches per SLA; re-verify Covered List quarterly.

• Reassessment: Tier 1 annually, Tier 2 every 18–24 months, Tier 3 on trigger events, Tier 4 on initial assessment.

11. Bill of Materials (BOM) & Software Bill of Materials (SBOM)

Pioneer Telephone Cooperative establishes requirements for supply chain transparency, component visibility, and product integrity verification across the lifecycle of hardware, software, firmware, and services used by the Cooperative. Its purpose is to provide a clear understanding of the components, dependencies, sources, and potential risks associated with products deployed within the organization's environment.

By requiring Software Bills of Materials (SBOMs), Hardware Bills of Materials (HBOMs), supplier provenance attestations, and component inventory records, Pioneer gains the ability to identify vulnerable, counterfeit, tampered, unsupported, or high-risk components that may impact the security, reliability, or resilience of critical systems and services. The section also establishes processes for reviewing component information, monitoring supplier integrity, and validating the authenticity of products obtained through the supply chain.

These practices enhance Pioneer’s ability to respond to emerging vulnerabilities, comply with regulatory and grant requirements, strengthen supplier accountability, and reduce risks associated with software dependencies, hardware sourcing, counterfeit products, and supply chain attacks. By maintaining visibility into the components that support business operations and customer services, the Cooperative improves its overall cybersecurity posture and supply chain resilience. The practices include:

• Software Bill of Materials (SBOM) Requirements: Suppliers providing software, firmware, cloud applications, or embedded systems shall provide a current SBOM in SPDX or CycloneDX format for all major releases and significant updates. SBOMs shall identify software components, versions, dependencies, suppliers, and known vulnerabilities.

• Hardware Bill of Materials (HBOM) Requirements: Suppliers providing hardware or network infrastructure shall provide, upon request, identifying critical components, manufacturers, country of origin, and supply-chain dependencies necessary to assess sourcing and integrity risks.

• Supplier Attestation of Integrity and Provenance: Suppliers shall annually attest that delivered products have been developed, manufactured, stored, and transported through authorized channels and have not been knowingly modified, tampered with, or substituted during the supply chain process.

• Component Inventory Management: Pioneer Telephone Cooperative shall maintain an inventory of critical third-party hardware, software, firmware, and services used in production environments. Inventory records shall include supplier information, version information, SBOM/HBOM references where available, support status, and identified supply-chain risks.

• SBOM/HBOM Review Process: Engineering / Network Manager shall review SBOMs and HBOMs during initial procurement, major upgrades, and periodic risk assessments to identify vulnerable, counterfeit, unsupported, or high-risk components.

• Supply Chain Monitoring: For Tier 1 and other critical suppliers, Pioneer shall monitor supplier security posture, vulnerability disclosures, sanctions, ownership changes, and other indicators of supply-chain risk. Where feasible and commensurate with risk, suppliers may be required to provide visibility into manufacturing controls, secure development practices, and product integrity controls.

• Counterfeit and Tampering Detection: Vendors shall maintain controls designed to prevent, detect, and report counterfeit components, unauthorized substitutions, tampering, and other integrity violations. Evidence of such controls shall be provided upon request.

• Risk-Based Verification: Pioneer may perform validation activities including supplier questionnaires, independent assessments, review of assurance reports, product authenticity verification, and evaluation of software signing mechanisms to confirm component integrity.

12. Acquisition & Receiving Controls

Pioneer Telephone Cooperative establishes the controls used to verify the authenticity, integrity, and compliance of products and equipment before they are accepted into the Cooperative's environment. Its purpose is to reduce the risk of counterfeit, tampered, unauthorized, or non-compliant products entering the organization's network and operational infrastructure.

The controls require verification of approved suppliers and regulatory compliance prior to purchase, validation of product integrity during shipping and receipt, and technical testing before equipment is placed into production. By maintaining chain-of-custody records,

documenting receiving activities, and verifying firmware authenticity and security configurations, Pioneer helps ensure that acquired products meet organizational security requirements and have not been altered or compromised during manufacturing, transportation, or storage.

These practices support supply chain transparency, regulatory compliance, asset accountability, and the secure deployment of hardware and software used to deliver critical telecommunications and broadband services. Requirements may include:

• Verify APL and FCC Covered List status before PO; retain verification snapshot with PO records.

• Secure shipping, tamper-evident seals; capture serials at receipt; photographic evidence of packaging condition.

• Acceptance testing: verify firmware images and signatures; apply baseline secure configurations before production.

13. Operational Controls & Monitoring

Pioneer Telephone Cooperative establishes the operational security controls and continuous monitoring activities used to protect the Cooperative's systems, networks, and assets from supply chain-related threats throughout their operational lifecycle. Its purpose is to ensure that equipment, software, and services obtained through the supply chain remain secure, properly managed, and compliant after deployment.

These controls provide ongoing visibility into organizational assets, configurations, vulnerabilities, and security events, enabling Pioneer to identify and respond to potential risks before they impact business operations or customer services. By maintaining accurate asset inventories, enforcing secure configuration standards, monitoring for vulnerabilities, and collecting centralized security telemetry, the organization strengthens its ability to detect compromised products, unauthorized changes, malicious updates, and other supply chain security concerns.

This continuous monitoring approach supports operational resilience, regulatory compliance, incident response, and effective risk management while helping ensure the confidentiality, integrity, and availability of critical telecommunications and broadband services. Requirements may include:

• Maintain authoritative asset inventory with model/serial, firmware, SBOM link, tier, and location.

• Configuration management and golden images; disable insecure services; unique credentials and PKI enrollment.

• Continuous vulnerability scanning and exposure management tied to patch SLAs by severity.

• Centralized logging/telemetry to SIEM; detections for supply-chain indicators (e.g., unexpected beacons, unsigned updates).

14. Incident Response & Remediation (Supply Chain Events)

Pioneer Telephone Cooperative establishes the processes and responsibilities for identifying, responding to, and recovering from cybersecurity incidents and disruptions originating from suppliers, service providers, software vendors, hardware manufacturers, or other third parties within the supply chain. Its purpose is to minimize the operational, security, and customer impacts of supply chain-related incidents while ensuring timely containment, remediation, and recovery actions.

The section provides a structured approach for investigating supply chain threats, coordinating response activities with affected suppliers, isolating impacted systems, and implementing corrective actions to restore secure operations. It also ensures that indicators of compromise, remediation activities, and supporting evidence are properly documented to support regulatory, legal, contractual, and grant compliance requirements.

By establishing predefined response procedures and playbooks for common supply chain events, Pioneer Telephone Cooperative improves its ability to detect and respond to supplier-related cybersecurity incidents, reduce the risk of service disruptions, protect critical telecommunications and broadband infrastructure, and maintain the trust of customers, regulators, and stakeholders. Requirements may include:

• Triage supply chain alerts; coordinate with vendor; block suspicious updates; isolate affected assets.

• Document IOCs and eradication steps; use emergency change windows for critical fixes; customer communications as needed.

• Remove/replace equipment that becomes prohibited or unsupported; maintain evidence for grant compliance.

• Use playbooks for device compromise, unauthorized update channels, or supplier breach impacting Cooperative systems.

15. Review, Maintenance, and Attestation

This plan is reviewed at least annually and upon significant changes (e.g., major supplier changes, critical vulnerabilities, regulatory updates). Updates are approved by the GM and Board. Attestations required under BEAD are prepared and submitted by the CISO or designee within required timelines.

Appendix A – Required Contract Clauses

• Prohibition on Covered Equipment/Services: Supplier warrants that no products/services in this agreement are on the FCC Covered List and shall notify within 24 hours if status changes.

• SBOM and VEX: Supplier shall provide SBOMs (SPDX/CycloneDX) for each major/minor release and update VEX within 10 business days of new CVEs.

• Security Incident Notice: Supplier shall notify within 24–48 hours of confirmed incidents affecting supplied products/services and provide IOCs and mitigations.

• Right to Audit: For Tier 1 suppliers, customer may conduct audits or accept recent independent assurance reports (e.g., SOC 2, ISO 27001).

• Access Controls & Logging: MFA for administrative access; least privilege; logging with retention; provide logs upon request.

• Data Protection & Residency: Encryption in transit/at rest; data location disclosure and restrictions as required.

• Sub-supplier Oversight: Supplier maintains oversight of critical sub-suppliers and discloses material changes.

• Business Continuity: Maintain BCP/DR with RTO/RPO targets for critical services and disclose alternate sites.