IS CYBERSECURITY PROCUREMENT REQUIREMENTS

Title: [Enter Project or RFP/RFQ Name]

Dated: [Date]

Pursuant to Agreement # 560_____

ABOUT CANADIAN PACIFIC

Canadian Pacific Railway Company (TSX:CP)(NYSE:CP) ("**CPR**") is a transcontinental railway operating in Canada and the United States providing North American customers a competitive rail service with access to key markets in every corner of the globe. CPR is growing with its customers, offering a suite of freight transportation services, logistics solutions and supply chain expertise. Visit www.cpr.ca for additional information on CPR.

Scope:

The IS Cybersecurity Procurement Requirement document provides minimum cybersecurity practices that are required to reduce cybersecurity risks and challenges that the procurement and use of a Supplier's products or services could pose to Canadian Pacific Railway Company ("**CPR**") and/or its affiliates. Suppliers must use this document as a guide to align their practices accordingly. These requirements pertain to the procurement of products, including:

1. **Application Software** or **Industrial Control System (ICS)**, including individual railroad systems (e.g., a SCADA system, etc.).
2. **Application Software** or I**ntegrated Solutions**, including Information Technology ("**IT**") systems and/or services that support business operations, including application systems, embedded software, firmware, drivers, middleware and operating systems, partly or wholly sourced and implemented for CPR by Suppliers;
3. **Industrial Control System (ICS),** e.g., individual components of railroad systems (e.g., programmable logic controllers, digital relays, or remote terminal units).
4. **Integrated Solutions**, including:
    a. Integrated, assembled or networked railroad systems (e.g. back office or operational systems, for example on locomotives or wayside installations).
    b. Associated services, including Suppliers of services for railroad systems (e.g., consulting, support and maintenance activities).
5. **Cloud Solutions**, e.g. outsourced services, including services provided by Cloud Service Providers (CSP);

Unless otherwise specified, in a Transactional document the requirements identified in this document applies "at the point of delivery" of the product and/or service (i.e. prior to acceptance). However, documentation requested to support requirements will be due when the Supplier submits a response.

A CPR IT Project or RFP/RFQ Name must be identified and included as part of the Supplier's response.

Other factors that Supplier should identify in the response:

- Best of class services and/or offerings that CPR may not have considered or identified; and,
- Any restrictions (legal, logistical, etc.) for Supplier to provide these Services in the US or Canada.

Contents of this document:

1. Applicability table
2. Section 1 - Supplier's Cybersecurity Program
3. Section 2 - Cybersecurity Technical Requirements System Hardening
4. Section 3 - Independent Attestation and Validation/Certification of Cybersecurity Requirements
5. Section 4 - Abbreviations & Definitions
6. Section 5 – Cybersecurity Requirement Compliance Matrix
7. Section 6 – Letter from Supplier to CPR

Contact

The Supplier shall make all questions, inquiries or clarifications regarding these Cybersecurity Requirements in writing to the Contact Person:

FORWARD YOUR REPLY AND DOCUMENTS TO:
Enter [Title] ("**Contact Person**")
Canadian Pacific Railway Company ("CPR")
7550 Ogden Dale Road S.E. BLDG #1
Calgary, Alberta, Canada, T2P 4Z4
Phone: 403.319XXX
E-Mail: **[e-mail**

SCHEDULE OF EVENTS

Major events in the process, and applicable deadline dates.

Key Event	Deadline Date
Cybersecurity Requirements Issued	**[Enter date and time]**
Proponent Cybersecurity Requirements questions deadline	**[Enter date and time]**
CPR Responses	**[Enter date and time]**
Cybersecurity Requirements Response Due Date	**[Enter date and time]**
Discussion of Cybersecurity Responses	**[Enter date and time]**

Applicability Table:

Select applicable requirements below:	Application Software	Integrated Solution	ICS	Cloud Solution
1. Supplier's Cybersecurity Program				
1.1 Secure Systems Development Practices	1.1.1 - 1.1.7	1.1.8 - 1.1.14		
1.2 Documentation and Tracking of Vulnerabilities and Notification of Cybersecurity Breaches	1.2.1 - 1.2.2	1.2.3 - 1.2.5		
1.3 Problem Reporting	1.3.1 - 0	1.3.3 - 1.3.5		
1.4 Patch Management and Updates	1.4.1	1.4.2 - 1.4.5		
1.5 Personnel Background Checks	1.5.1 - 1.5.3	1.5.4 - 1.5.7		
1.6 Secure Hardware and Software Delivery	1.6.1 - 1.6.3	1.6.4 - 1.6.7		
2. Cybersecurity Technical Requirements				
2.1. System Hardening	2.1.1 – 2.1.6	2.1.7 – 2.1.12		
2.2. Access Control	2.2.1 – 2.2.7	2.2.8 – 2.2.14		
2.3. User Account Management	2.3.1 – 2.3.3	2.3.1– 2.3.7		
2.4. Application Session Management	2.4.1 – 2.4.4	2.4.5 – 2.4.8		
2.5. Authentication/Password Policy and Mgmt.	2.5.1 – 2.5.5	2.5.6 – 2.5.10		
2.6. Logging and Auditing	2.6.1 – 2.6.7	2.6.8 – 2.6.14		
2.7. Communication Restrictions	2.7.1 – 2.7.11	2.7.12 – 2.7.26		
2.8. Malware Detection and Protection	2.8.1	2.8.2 – 2.8.3		
2.9. Intrusion Detection	2.9.1	2.9.2 – 2.9.3		
2.10. Cryptographic System Management	2.10.1 – 2.10.2	2.10.3 – 2.10.4		
2.12. Wireless Technologies	2.11.1 – 2.11.8	2.11.9 – 2.11.17		
2.13. Software Patching	2.12.1 – 2.12.2	2.12.3 – 2.12.5		
2.14. Backup	2.13.1	2.13.2 – 2.13.3		
2.15. Software License Management	2.14.1	2.14.2		
3. Independent Attestation & Validation/Certification of Cybersecurity Requirements				
3.1. Independent Attestation	3.1.3 – 3.1.2	3.1.3 – 3.1.4		3.1.3 – 3.1.4
3.2. Validation for ICS Related Products/Services			3.2.1 – 3.2.5	
3.3. Validation for IT Procured Products/Services	3.3.1 – 3.3.2	3.3.3 – 3.3.4		3.3.3 – 3.3.4

Notes:

Application Software: Standalone software provided by Suppliers that will be implemented by CPR.

Integrated Solution: A third party Supplier solution which includes several hardware and software components from different Suppliers implemented as a single integrated solution.

ICS: Industrial control system.

Requirements:

Section 1 - Supplier's Cybersecurity Program

1. Supplier's Cybersecurity Program

Cybersecurity program and associated practices are important considerations in the procurement process as vulnerabilities frequently result from insecure architecture and/or design weaknesses, vulnerabilities in hardware, software, and firmware coding, as well as in bundled third-party products.

1.1. Secure Systems Development Practices

Secure product development practices are a set of processes integrated into the system development life cycle (SDLC) to reduce cybersecurity risks.

Application Software:
The Supplier shall ensure:

1.1.1 That they adhere to Systems Development Life Cycle (SDLC) best practices in developing their software solution.

1.1.2 That the origin of the procured product and its components (including hardware, software, and firmware) is not from a country that the Unites States and/or Canada has imposed embargoes and economic sanctions.

1.1.3 That the software and firmware of the procured product undergoes quality control and cybersecurity tests (which includes common test for the most common vulnerabilities and exploits) to identify and correct potential functional defects and cybersecurity weaknesses and vulnerabilities.

1.1.4 Maintenance of coding reviews, including defect lists and plans to correct identified vulnerabilities.

1.1.5 That a single technical point of contact (e.g., a company support email address or a company support phone number), for security-related technical issues. Maintain a continuous line of communication with CPR representatives.

1.1.6 Maintenance of a contingency plan for sustaining the security of the procured product, in the event the Supplier leaves the business.

1.1.7 Maintenance of appropriate documentation of its cybersecurity program, including any recent security assessment results. At CPR's request, an independent CPR approved third party will conduct these security assessments.

Integrated Solution, Cloud Solution & ICS:
The Supplier shall:

1.1.8 Provide a written summary of its SDLC including the standards, practices (including continuous improvement), and development environment (including the use of secure coding practices) used to create or modify Supplier-provided solution/system.

1.1.9 Identify the country (or countries) of origin (which includes development, manufacturing, maintenance, and service) of the procured solution and its components (including hardware, software, and firmware), ensuring they are not from a country that the Unites States and/or Canada has imposed embargoes and economic sanctions against. The Supplier shall notify CPR of changes in the list of countries to the point of

"delivery" of the product and/or service and shall be performed, prior to initiating a change in the list of countries.

1.1.10 Provide documentation of its quality assurance program and validate that the software and firmware of the procured solution have undergone quality control and cybersecurity testing (which includes common test for the most common vulnerabilities and exploits) to identify and correct functional defects as well as cybersecurity weaknesses and vulnerabilities. At CPR's request, this testing will be performed by a CPR approved independent entity. The Supplier shall provide a written summary of the test results, including unresolved vulnerabilities and recommended mitigation measures.

1.1.11 Provide a written summary of its coding reviews, including defect lists and where applicable, plans to correct identified vulnerabilities for the procured solution and associated components.

1.1.12 Identify a single technical point of contact (e.g., a company support email address or a company support phone number), for security-related technical issues. Maintain a continuous line of communication with CPR representatives.

1.1.13 Provide a contingency plan for the security of the procured solution in the event the Supplier leaves the business (e.g., security-related procedures and products placed in escrow).

1.1.14 Provide documentation of its implemented cybersecurity program, including any recent security assessment results. At CPR's request, a CPR approved independent third party will conduct a security assessment.

1.2 Documentation and Tracking of Vulnerabilities and Notification of Cybersecurity Breaches

The discovery of security vulnerabilities in hardware, software, and firmware, requires the timely application of corrective actions and/or mitigating steps that will reduce the likelihood vulnerabilities will be exploited.

Application Software:

The Supplier shall:

1.2.1 Ensure that disclosed vulnerabilities in the procured product are remediated prior to implementation at CPR, so that the procured product is delivered free of software vulnerabilities. For vulnerabilities discovered at the point of delivery, the Supplier shall provide a status of disposition for each vulnerability, with timelines for remediation.

1.2.2 Disclose, within a reasonable period of time, any cybersecurity breaches involving the Supplier, the procured product or its supply chain. Disclosure shall include a description of the breach, its potential security impact, its root cause, and the implemented, or planned, corrective action(s).

Integrated Solution, Cloud Solution & ICS:

The Supplier shall:

1.2.3 Provide, prior to the delivery of the procured solution, a written summary of vulnerabilities in the procured solution and the status of disposition of vulnerabilities accordingly.

1.2.4 Provide, within a reasonable period of time and after product delivery, a summary of uncorrected security vulnerabilities in the procured solution. This summary shall include information on vulnerabilities that have not been publicly disclosed or have only been identified after the delivery of the product. This documentation shall include a description of each vulnerability and its potential impact, root cause, and recommended compensating security controls, mitigation measures, and/or procedural workarounds.

1.2.5 Supplier shall notify CPR and shall provide a written summary within 72 hours of knowing of a cybersecurity breach(es) involving the Supplier, the procured solution or its supply chain. Initial and follow-up documentation shall include a description of the breach, its potential security impact, its root cause, and recommended corrective actions involving the procured solution.

1.3 Problem Reporting

A vulnerability mitigation process allows for the tracking of progress to develop workarounds, patches, and fixes. Timely notification of vulnerabilities is essential to create defenses for zero-day exploits.

Application Software:
The Supplier shall:

1.3.1 Maintain a secure and auditable process for users to submit problem reports (including potential bugs) and remediation requests. This process shall include tracking history and corrective action status reporting.

1.3.2 Maintain responsible disclosure and threat reporting policies and procedures (e.g., Computer Emergency Response Teams [CERTs]), to address public disclosure protections.

Ensure that upon the receipt of a problem report, the Supplier will review the report, develops an initial action plan within a reasonable period of time, and provide problem resolution status reports to CPR.

Integrated Solution, Cloud Solution & ICS:
The Supplier shall:

1.3.3 Provide a secure process for users to submit problem reports (including potential bugs) and remediation requests for the procured solution. This process shall include tracking history and corrective action status reporting.

1.3.4 Provide CPR with its responsible disclosure and threat reporting policies and procedures (e.g., Computer Emergency Response Teams [CERTs]), to address public disclosure protections.

1.3.5 Upon receiving of a problem report, review and develop an initial action plan within a reasonable period of time, and provide a status report of the problems resolution to CPR.

1.4 Patch Management and Updates

The discovery of product weaknesses and vulnerabilities is an ongoing process. To remediate discovered weaknesses and vulnerabilities, responsible system and product Supplier must

regularly release updates, patches, service packages, or other fixes to their products—including third- party hardware, software, and firmware. Testing and validation of the patches and upgrades are necessary prior to performing the updates on a production system.

Application Software:
The Supplier shall:

1.4.1 Maintain a patch management program and update process (including any third-party hardware, software, and firmware). This program shall:
- 1.4.1.1 Include the a process for validating the integrity of the patch;
- 1.4.1.2 Address zero-day vulnerabilities;
- 1.4.1.3 Ensure that updates to remediate vulnerabilities or weaknesses are provided within two weeks of the vulnerability becoming public, or based on a support agreement;
- 1.4.1.4 Ensure that updates to remediate critical vulnerabilities are provided within a shorter period than other updates;

Integrated Solution, Cloud Solution & ICS:
The Supplier shall:

1.4.2 Provide documentation relating to its patch management program and update process (including third-party hardware, software, and firmware). This shall include the Supplier's method (or recommendation) for validating the integrity of the patch

1.4.3 Clarify how its patch management program addresses zero-day vulnerabilities.

1.4.4 Provide documentation that procured products (including third-party hardware, software, firmware, and services) have appropriate updates and patches installed prior to delivery to CPR.

1.4.5 Provide all updates to remediate critical vulnerabilities within one week of the critical vulnerability becoming public. If updates cannot be made available by the Supplier within these period of time, the Supplier shall provide mitigations and/or workarounds within accordingly

1.5 Supplier Personnel Management

Supplier personnel who have access, or will be granted access to CPR's systems, or have sensitive information about the system, need to protect this information from adversaries. Without consistent Supplier personnel management processes, sensitive information and access to assets can be compromised when changes to a Supplier's staff occurs.

Application Software:
The Supplier shall:

1.5.1 Maintain a well-documented cybersecurity training and awareness program, to provide ongoing reinforcement in good cybersecurity practices, to its workforce, especially those involved in the design, development, manufacture, testing, shipping, installation, operation, and maintenance of products procured by CPR.

1.5.2 Maintain a well-documented consistent process to perform security background checks on its employees (including contracted personnel) working directly on or involved in the development of a CPR system or procured product.

1.5.3 Maintain consistent well-documented processes to ensure that policies and procedures are followed to prohibit the unauthorized disclosure of knowledge, information, architectures, or configuration relevant to CPR's system.

Integrated Solution, Cloud Solution & ICS:
The Supplier shall:

1.5.4 Provide a written summary of its cybersecurity training and awareness program, for those involved in the design, development, manufacture, testing, shipping, installation, operation, and maintenance of solutions procured by CPR.

1.5.5 Perform security background checks on its employees (or contracted personnel) working directly on, or involved in, the development of a CPR system or procured solution.

1.5.6 Provide documented evidence that policies and procedures are adhered to in order to prohibit the unauthorized disclosure of knowledge, information, architectures, or configuration relevant to CPR's systems.

1.5.7 Demonstrate that they perform timely updates to user/system authentication credentials and access controls, based on relevant staffing changes.

1.6 Secure Hardware and Software Delivery

Information and Communications Technology (ICT) supply chain is complex and extended, and it provides numerous opportunities for subversion, including malicious code insertion, counterfeit insertion, and tampering. Specifically, information and communications technology, requires protection during delivery, both physically (when components are transported) and logically (when software, including patches, are downloaded).

Application Software:
The Supplier shall:

1.6.1 Maintain a risk management process, for its information and communications technology supply chain delivery of hardware, software, and firmware. The process shall include at a minimum:

1.6.1.1 Chain-of-custody practices;

1.6.1.2 Inventory management program (including the location and protection of spare parts);

1.6.1.3 Information protection practices;

1.6.1.4 Integrity management program for components provided by sub-Suppliers;

1.6.1.5 Instructions on how to request replacement parts;

1.6.1.6 Maintenance commitment to ensure that for a specified time into the future, spare parts shall be made available by the Supplier;

1.6.2 Maintain, where applicable, a digital delivery process for procured products (e.g., software and data) to ensure the digital delivery is adequately protected.

1.6.3 Maintain processes for detecting unauthorized access throughout the delivery of the procured product.

Integrated Solution, Cloud Solution & ICS:
The Supplier shall:

1.6.4 Provide documentation of its risk management process, for its information and communications technology supply chain delivery of hardware, software, and firmware. The process shall include at a minimum:

1.6.4.1 Chain-of-custody practices;

1.6.4.2 Inventory management program (including the location and protection of spare parts, where appropriate);

1.6.4.3 Information protection practices;

1.6.4.4 Integrity management program for components provided by sub-Suppliers;

1.6.4.5 Instructions on how to request replacement parts;

1.6.4.6 Maintenance commitment to ensure that for a specified time into the future, spare parts shall be made available by the Supplier;

1.6.5 Provided documentation on how digital delivery for procured solutions (e.g., software and data) will be secured, validated and monitored to ensure the digital delivery is not compromised.

1.6.6 Provided documentation regarding the use of trusted channels to ship critical railroad system hardware, such as registered mail.

1.6.7 Provide documentation of its capability for detecting unauthorized access throughout the delivery process.

1.6.8 Provide documentation of its chain-of-custody for critical railroad system hardware and require tamper-evident packaging for the delivery of this hardware

2. Cybersecurity Technical Requirements System Hardening

Application Software:

The Supplier shall:

2.1.1. Provide a documented process that will allow CPR to remove/disable all software components that are not required for the operation and/or maintenance of the procured product, without impeding the primary function of the procured product. If unrequired software cannot be removed or disabled, the Supplier shall provide risk mitigating recommendations and/or countermeasures. The software to be removed and/or disabled includes:

- 2.1.1.1. Games
- 2.1.1.2. Device drivers for product components not procured/delivered
- 2.1.1.3. Messaging services (e.g., email, instant messenger, peer-to-peer file sharing)
- 2.1.1.4. Source code
- 2.1.1.5. Software compilers in user workstations and servers
- 2.1.1.6. Software compilers for programming languages that are not used in the railroad system
- 2.1.1.7. Unused networking and communications protocols
- 2.1.1.8. Unused administrative utilities, diagnostics, network management, and system management functions
- 2.1.1.9. Backups of files, databases, and programs used only during system development
- 2.1.1.10. All unused data and configuration files

2.1.2. Provide documentation of software/firmware that supports the procured product, including scripts and/or macros, run time configuration files and interpreters, databases and tables, and all other included software (identifying versions, revisions, and/or patch levels, as delivered). The listing shall include all ports and authorized services required for normal operation, emergency operation, or troubleshooting.

2.1.3. Provide a documented process for CPR to remove and/or disable (or provide documentation as to how it would be performed), through software, physical disconnection, or engineered barriers, services and/or ports in the procured product, not required for normal operation, emergency operations, or troubleshooting. This shall include communication ports and physical input/output ports (e.g., USB docking ports, CD/DVD drives, video ports, and serial ports). The Supplier shall provide documentation of disabled ports, connectors, and interfaces.

2.1.4. Provide a documented process for CPR to re-enable disabled ports and/or services if required at any time.

2.1.5. Disclose in writing the existence of all methods for bypassing authentication in the procured product, often referred to as backdoors, and provide written documentation that all such backdoors created by the Supplier or its Supplier have been permanently removed from the system.

2.1.6. Provide a summary of the procured product's cybersecurity features and security-focused instructions on product maintenance, support, and reconfiguration of default settings.

Integrated Solution, Cloud Solution & ICS:

The Supplier shall:

2.1.7. Remove all software components that are not required for the operation and/or maintenance of the procured solution. If removal is not technically feasible, then the Supplier shall disable software not required for the operation and/or maintenance of the procured solution. This removal shall not impede the primary function of the procured solution. If unrequired software cannot be removed or disabled, the Supplier shall document a specific explanation and provide risk-mitigating recommendations as to how they would be addressed. The software to be removed and/or disabled shall include, but not be limited to:

- 2.1.7.1. Games
- 2.1.7.2. Device drivers for product components not procured/delivered
- 2.1.7.3. Messaging services (e.g., email, instant messenger, peer-to-peer file sharing)
- 2.1.7.4. Source code
- 2.1.7.5. Software compilers in user workstations and servers
- 2.1.7.6. Software compilers for programming languages that are not used in the railroad system
- 2.1.7.7. Unused networking and communications protocols
- 2.1.7.8. Unused administrative utilities, diagnostics, network management, and system management functions
- 2.1.7.9. Backups of files, databases, and programs used only during system development
- 2.1.7.10. All unused data and configuration files

2.1.8. Provide documentation of software/firmware that supports the procured solution, including scripts and/or macros, run time configuration files and interpreters, databases and tables, and all other included software (identifying versions, revisions, and/or patch levels, as delivered). The listing shall include ports and authorized services required for normal operation, emergency operation, or troubleshooting.

2.1.9. Remove and/or disable (or provide documentation as to how it would be performed), through software, physical disconnection, or engineered barriers, all services and/or ports in the procured product not required for normal operation, emergency operations, or troubleshooting. This shall include communication ports and physical input/output ports (e.g., universal serial bus (USB) docking ports, CD/DVD drives, video ports, and serial ports). The Supplier shall provide documentation of disabled ports, connectors, and interfaces.

2.1.10. Configure the procured product to allow CPR to re-enable ports and/or services if they are disabled by software.

2.1.11. Demonstrate that all methods for bypassing authentication in the procured product, often referred to as backdoors, created by the Supplier or its Supplier have been permanently removed from the system.

2.1.12. Provide a written summary of the procured product's security features and security-focused instructions on product maintenance, support, and reconfiguration of default settings.

2.2. Access Control

Application Software:

The Supplier shall provide capabilities to:

2.2.1. Configure each component of the procured product to operate using the principle of least privilege, including operating system permissions, file access, user accounts, application-to-application communications, and railroad system services.

2.2.2. Modify user accounts with configurable access and permissions associated with one or more organizationally defined user role(s), where roles are used, and to change user(s') role (e.g., group) associations.

2.2.3. To protect against unauthorized privilege escalation.

2.2.4. To define access and security permissions, user accounts, and applications with associated roles.

2.2.5. To prevent unauthorized changes to the Basic Input/output System (BIOS) and other firmware. If it is not technically feasible to protect the BIOS to reduce the risk of unauthorized changes, the Supplier shall document this case and provide mitigation recommendations.

2.2.6. Identify the unauthorized installation of logging devices (e.g., key loggers, cameras, and microphones).

2.2.7. The Supplier shall deliver a product that enables CPR to configure its components to limit access to and from specific locations (e.g., security zones, business networks, and demilitarized zones [DMZs]) on the network to which the components are attached, where appropriate, and provide CPR with the documentation of the delivered product's configuration

Integrated Solution, Cloud Solution & ICS:

The Supplier shall:

2.2.8. Configure each component of the procured solution to operate using the principle of least privilege, including operating system permissions, file access, user accounts, application-to-application communications, and railroad system services.

2.2.9. Provide user accounts with configurable access and permissions associated with one or more organizationally defined user role(s), where roles are used. The Supplier shall provide a system administration mechanism for changing user(s') role (e.g., group) associations.

2.2.10. Provide a method for protecting against unauthorized privilege escalation.

2.2.11. Document options for defining access and security permissions, user accounts, and applications with associated roles. The Supplier shall configure these options, as specified by CPR accordingly.

2.2.12. Recommend methods to prevent unauthorized changes to the Basic Input/output System (BIOS) and other firmware. If it is not technically feasible to protect the BIOS to reduce the risk of unauthorized changes, the Supplier shall document this case and provide mitigation recommendations.

2.2.13. Identify and provide documentation relating to the procured solution, attesting that there are no unauthorized installation of logging devices (e.g., key loggers, cameras, and microphones).

2.2.14. Deliver a solution that enables CPR to configure its components to limit access to and from specific locations (e.g., security zones, business networks, and demilitarized zones

[DMZs]) on the network to which the components are attached, where appropriate, and provide CPR with the documentation of the delivered product's configuration.

2.3. User Account Management

Application Software:

The Supplier shall provide capabilities to:

2.3.1. Change default account settings to CPR-specific settings (e.g., length, complexity, history, and system privileges) or provide support to CPR in these changes.

2.3.2. Remove or disable any unnecessary accounts for normal or maintenance operations of the software.

2.3.3. Where applicable, the Supplier shall, place emergency operations accounts in a highly secure configuration, and provide CPR with that documentation.

Integrated Solution, Cloud Solution & ICS:

The Supplier shall:

2.3.4. Document all accounts (including, but not limited to, generic and/or default) that need to be active for proper operation of the procured product.

2.3.5. Change default account settings to CPR-specific settings (e.g., length, complexity, history, and configurations) or provide support to CPR in these changes. The Supplier shall provide new account information to CPR via a protected mechanism.

2.3.6. Remove or disable any unnecessary accounts for normal or maintenance operations of the solution, prior to the delivery of the procured solution.

2.3.7. Where applicable, place emergency operations accounts in a highly secure configuration, and provide CPR with that documentation

2.4. Application Session Management

Application Software:

The Supplier shall provide imbedded capabilities to:

2.4.1. Restrict user credentials from being stored, transmitted or shared in clear text. The Supplier shall allow secure access protocols that encrypt or securely transmit login credentials (e.g., tunneling through Secure Shell Terminal Emulation [SSH], Transport Layer Security [TLS]).

2.4.2. Configure an appropriate level of protection (e.g., encryption and digital signing) for the application and control system sessions, in accordance with internationally acceptable standards, commensurate with the technology platform, communications characteristics, and response time constraints.

2.4.3. Configure software systems to disallow multiple concurrent logins using the same authentication credentials.

2.4.4. Provide account-based and group-based configurable session-based logout and timeout settings (e.g., alarms and human-machine interfaces).

Integrated Solution, Cloud Solution & ICS:

The Supplier shall:

2.4.5. Ensure that user credentials, in the procured solution, are not stored, transmitted or shared in clear text. The Supplier shall allow secure access protocols that encrypt or securely

transmit login credentials (e.g., tunneling through Secure Shell Terminal Emulation [SSH], Transport Layer Security [TLS]).

2.4.6. Configure an appropriate level of protection (e.g., encryption and digital signing) for the application and control system sessions, in accordance with CPR enterprise security standards and directives, commensurate with the technology platform, communications characteristics, and response time constraints.

2.4.7. Configure software systems to disallow multiple concurrent logins using the same authentication credentials.

2.4.8. Provide account-based and group-based configurable session-based logout and timeout settings (e.g., alarms and human-machine interfaces).

2.5. Authentication/Password Policy and Management

Application Software:

The Supplier shall:

2.5.1. Deliver a product that uses secure Industry standard (internationally acceptable) authentication protocols.

2.5.2. Implement mechanisms to protect passwords, including not storing passwords in clear text and not hardcoding passwords into software or scripts.

2.5.3. Ensure that If needed for ongoing support and maintenance, the procured product's interactive remote access/control support's (i.e., be compatible with) CPR's implementation of multifactor authentication (e.g., two-factor or token).

2.5.4. Provide a configurable account password management system that allows for, but is not limited to, the following:

i. Changes to passwords (including default passwords)
ii. Selection of password length
iii. Frequency of change
iv. Setting of required password complexity
v. Number of login attempts prior to lockout
vi. Inactive session logout
vii. Screen lock by application
viii. Comparison to a library of forbidden strings
ix. Derivative use of the user name
x. Denial of repeated or recycled use of the same password

2.5.5. Provide a centralized local account management capability.

Integrated Solution, Cloud Solution & ICS:

The Supplier shall:

2.5.6. Deliver a solution that uses secure standard authentication protocols.

2.5.7. Implement mechanisms to protect passwords, including not storing passwords in clear text and not hardcoding passwords into software or scripts.

2.5.8. Ensure that If needed for ongoing support and maintenance, the procured product's interactive remote access/control support's (i.e., be compatible with) CPR's implementation of multifactor authentication (e.g., two-factor or token).

2.5.9. Provide a configurable account password management system that allows for, but is not limited to, the following:

xi. Changes to passwords (including default passwords)
xii. Selection of password length
xiii. Frequency of change

xiv. Setting of required password complexity
xv. Number of login attempts prior to lockout
xvi. Inactive session logout
xvii. Screen lock by application
xviii. Comparison to a library of forbidden strings
xix. Derivative use of the user name
xx. Denial of repeated or recycled use of the same password

2.5.10. Provide a centralized and local account management capability.

2.6. Logging and Auditing

Application Software:
The Supplier shall:

2.6.1. Provide information about the procured product's logging capabilities. The procured product shall cover the following events, at a minimum (as appropriate to their function):
- Information requests and server responses
- Successful and unsuccessful authentication and access attempts
- Account changes
- Privileged use
- Application start-up and shutdown
- Application failures
- Major application configuration changes

2.6.2. Ensure that the procured product provides standard time synchronization capabilities in the procured product (e.g., Global Positioning System [GPS], Network Time Protocol [NTP], and IEEE 1508-2008), to synchronize to an authoritative time source.

2.6.3. Ensure that the procured product provides applies time stamps to audit trails and log files, as required by CPR enterprise security standards and directives.

2.6.4. Ensure that the procured product provides confidentiality and integrity security protection of log files.

2.6.5. Ensure that the procured product implements secure mechanisms for collecting and storing (e.g., transfer or log forwarding) security log files.

2.6.6. Ensure that the procured product provides log management capabilities for generating logs in internationally acceptable format. This list shall identify which of those logs are enabled by default.

2.6.7. Provide log and Security Information and Event Management (SIEM) integration methods (e.g., syslog) that is compatible with the procured product.

Integrated Solution, Cloud Solution & ICS:
The Supplier shall:

2.6.8. Provide information about the procured product's logging capabilities. The procured product shall cover the following events, at a minimum (as appropriate to their function):
- Information requests and server responses
- Successful and unsuccessful authentication and access attempts
- Account changes
- Privileged use
- Application start-up and shutdown
- Application failures

- Major application configuration changes

2.6.9. Ensure that the procured solution provides standard time synchronization capabilities (e.g., Global Positioning System [GPS], Network Time Protocol [NTP], and IEEE 1508-2008). If the Supplier is not providing standard time synchronization and is providing an authoritative time source, the procured product shall be configured to synchronize to the authoritative time source.

2.6.10. Ensure that the procured solution applies time stamps to audit trails and log files, as required by CPR enterprise security standards and directives.

2.6.11. Ensure that the procured solution provides confidentiality and integrity security protection of log files.

2.6.12. Ensure that the procured solution implements a secure approach for collecting and storing (e.g., transfer or log forwarding) security log files.

2.6.13. Ensure that the procured solution provides log management capabilities for generating logs in internationally acceptable formats. This list shall identify which of those logs are enabled by default.

2.6.14. Provide log management and Security Information and Event Management (SIEM) integration methods (e.g., syslog).

2.7. Communication Restrictions

Application Software:

The Supplier shall:

2.7.1. Provide documentation of ports and protocols in use and methods for isolating the system while continuing limited operations.

2.7.2. Provide documentation on all communications required between system components, if placed in different network security zones.

2.7.3. Provide documentation identifying each network component of the procured product initiating communication, and provide a method to restrict communication traffic between different network security zones.

2.7.4. Provide documentation on any method, or equipment that could be used to restrict communication traffic.

2.7.5. Provide documentation of all remote access entry pathways and ensure that they could be enabled or disabled by CPR as required.

2.7.6. Provide CPR with access, including administrative access as needed, to network components of the procured product, including firewalls.

2.7.7. Provide verification that the procured product and components allows the use of unique routable network address spaces (i.e., address spaces other than 192.168.0.0/16, 172.16.0.0/12, and 10.0.0.0/8 must be supported) that work within CPR's network. Where this is not available, the Supplier shall offer an alternative approach, with mitigating security measures, that is acceptable to CPR.

2.7.8. Configure the communication tunneling components of the procured product (e.g., connectors, filters, and concentrators) to provide end-to-end protection (e.g., end-to-end encryption) of the data in transit.

2.7.9. Provide a documented method for managing the network components of the procured product and changing configurations, including hardware and software configurations (e.g., addressing schemes).

2.7.10. Verify and provide documentation relating to the security of the network configuration management interface.

2.7.11. , Provide Access Control Lists (ACLs) for monitoring network components (e.g., port mirroring and network tap) of the procured product, where applicable.

Integrated Solution, Cloud Solution & ICS:

The Supplier shall:

2.7.12. Provide documentation of ports and protocols in use and methods for isolating the procured solution while continuing limited operations.

2.7.13. Provide documentation on all communications required between system components, if placed in different network security zones.

2.7.14. Provide documentation identifying each network component of the procured solution initiating communication, and provide a method to restrict communication traffic between different network security zones.

2.7.15. Provide documentation on any method or equipment used to restrict communication traffic and shall document the disconnection points established between network security zones.

2.7.16. Provide documentation on the firewalls and their firewall rule sets (If firewalls are provided) for normal and emergency operations. If CPR has the responsibility of procuring its own firewalls, the Supplier shall recommend appropriate firewall rule sets or rule set guidance for normal and emergency operations. The basis of the firewall rule sets shall be "deny all," with exceptions explicitly identified by the Supplier.

2.7.17. Provide document of all remote access entry pathways and ensure that they could be enabled or disabled by CPR as required.

2.7.18. Provide a means to document that network traffic is monitored, filtered, and alarmed (e.g., alarms for unexpected traffic through network security zones) and provide filtering and monitoring rules.

2.7.19. Provide CPR with access, including administrative access as needed, to network components of the procured product, including firewalls.

2.7.20. Provide verification that the procured product and components allows the use of unique routable network address spaces (i.e., address spaces other than 192.168.0.0/16, 172.16.0.0/12, and 10.0.0.0/8 must be supported) that work within CPR's network. Where this is not available, the Supplier shall offer an alternative approach, with mitigating security measures, that is acceptable to CPR.

2.7.21. Provide or utilize an existing security-isolated environment (for control systems) outside the control network (e.g., using a demilitarized zone [DMZ] or an equivalent or a superior form of security isolation) for the communications tunneling server to reside in.

2.7.22. Configure the communication tunneling components of the procured product (e.g., connectors, filters, and concentrators) to provide end-to-end protection (e.g., end-to-end encryption) of the data in transit.

2.7.23. Provide documentation relating to a method for managing the network components of the procured product and changing configurations, including hardware and software configurations (e.g., addressing schemes).

2.7.24. Provide documentation that verifies the security of the network configuration management interface.

2.7.25. Provide documentation relating to Access Control Lists (ACLs) for monitoring network components (e.g., port mirroring and network tap) of the procured product.

2.8. Malware Detection and Protection

Application Software:

The Supplier shall:

2.8.1. Provide validated documentation that the procured product, will not interfere with any cybersecurity services running on the same host with the procured product (e.g., virus checking and malware detection).

Integrated Solution, Cloud Solution & ICS:

The Supplier shall:

2.8.2. Provide documentation on how to implement the functionality to automatically scan and identify any removable media that found to exist in the procured solution.

2.8.3. Implement at least **one** of the following:

2.8.3.1. Provide a functionality to detect host-based malware. Quarantine (instead of automatically deleting) suspected infected files. Provide an updating scheme for malware signatures. Test and confirm compatibility of malware detection application patches and upgrades.

2.8.3.2. If the Supplier will not provide the host-based malware detection capability, then the Supplier shall suggest malware detection capabilities to be used and provide guidance on malware detection and configuration settings that will work with its products.

2.8.3.3. If the Supplier will not provide a host-based malware detection capability, nor suggest malware detection products, the Supplier shall provide an application whitelisting solution that is tested, validated, and documented that shall only permit approved applications to run on the procured solution.

2.8.3.4. The Supplier shall validate that cybersecurity services running on the procured solution (e.g., virus checking and malware detection) does not conflict with other such services running on the procured product.

2.9. Intrusion Detection

Application Software:

The Supplier shall:

2.9.1. Provide documented validation that the procured solution, will not interfere with any host intrusion detection system services running on the same host with the procured product.

Integrated Solution, Cloud Solution & ICS:

The Supplier shall:

2.9.2. Host Intrusion Detection System (HIDS):

2.9.2.1. Wherever applicable, provide either a configured HIDS or the information needed for CPR to configure the HIDS.

2.9.2.2. Wherever applicable, implement or recommend a configuration for the HIDS in a manner that adheres to requirements for CPR's operating system functions or business objectives.

2.9.2.3. Wherever applicable, apply the auditing and logging provisions outlined in Section 2.6 of this document to the HIDS.

2.9.3. Network Intrusion Detection System (NIDS):

2.9.3.1. Wherever applicable, recommend placement(s) nodes for the NIDS sensors to provide appropriate monitoring for the railroad system network.

2.9.3.2. Wherever applicable, shall provide traffic profiles with expected communication paths, network traffic, and expected utilization boundaries for behavior-based (also known as anomaly based) NIDS.

2.9.3.3. Wherever applicable, provide initial and routine update signatures for knowledge-based (also called signature-based) NIDS, or make provisions for CPR to obtain them directly.

2.9.3.4. Wherever applicable, provide either a configured NIDS or the information needed for CPR to configure the NIDS in adherence to CPR's functional requirements.

2.9.3.5. Provide a NIDS architecture that works with the procured solution's communication method.

2.10. Cryptographic System Management

Application Software:

2.10.1. Cryptographic System Documentation

The Supplier must:

2.10.1.1. Document how the cryptographic system protects the confidentiality, data integrity, authentication, and non-repudiation of devices and data flows in the underlying system. This documentation shall include, but not limited to, the following:

2.10.1.1.1. The cryptographic methods (hash functions, symmetric key algorithms, or asymmetric key algorithms) and primitives (e.g., Secure Hash Algorithm [SHA]- 256, Advanced Encryption Standard [AES]-128, RSA, and Digital Signature Algorithm [DSA]-2048) that are implemented in the procured product, and how these methods were implemented.

2.10.1.1.2. The preoperational and operational phases of key establishment, deployment, ongoing validation, and revocation.

2.10.1.1.3. Third party validated tests for cryptographic functions.

2.10.2. Cryptographic Key and Method Establishment, Usage, and Update

The Supplier must:

2.10.2.1. Provide certification or validation of the Use of "Approved" cryptographic methods as defined in the US National Institute of Standards and Technologies (NIST) Federal Information Processing Standard (FIPS) Security Requirements for Cryptographic Modules (FIPS 140-2).

2.10.2.2. Provide the automated remote key-establishment (update) method used in the procured product, that protects the confidentiality and integrity of the cryptographic keys.

2.10.2.3. Ensure that the procured product includes the capability for configurable Cryptoperiods (the life span of cryptographic key usage) in accordance with the Suggested Cryptoperiods for Key Types found in Table 1 of NIST 800-57 Part 1.

2.10.2.4. Ensure that the key update method used in the procured product, supports remote re-keying of all devices within a negotiated period of time(s) as part of normal system operations.

2.10.2.5. Ensure that emergency re-keying of all devices, in the procured product can be remotely performed within a negotiated period of time (e.g., 30 days).

2.10.2.6. Provide a method for updating cryptographic primitives or algorithms (updates to or replacement of the cryptographic method).

Integrated Solution, Cloud Solution & ICS:

2.10.3. Cryptographic System Documentation

The Supplier shall:

2.10.3.1. Document how the cryptographic system protects the confidentiality, data integrity, authentication, and non-repudiation of devices and data flows in the underlying system. This documentation shall include, but not limited to, the following:

2.10.3.1.1. The cryptographic methods (hash functions, symmetric key algorithms, or asymmetric key algorithms) and primitives (e.g., Secure Hash Algorithm [SHA]- 256, Advanced Encryption Standard [AES]-128, RSA, and Digital Signature Algorithm [DSA]-2048) that are implemented in the procured solution, and how these methods were implemented.

2.10.3.1.2. The preoperational and operational phases of key establishment, deployment, ongoing validation, and revocation.

2.10.3.1.3. Third party validated tests for cryptographic functions.

2.10.4. Cryptographic Key and Method Establishment, Usage, and Update

The Supplier shall:

2.10.4.1. Provide certification or validation of the Use of "Approved" cryptographic methods as defined in the US National Institute of Standards and Technologies (NIST) Federal Information Processing Standard (FIPS) Security Requirements for Cryptographic Modules (FIPS 140-2).

2.10.4.2. Provide the automated remote key-establishment (update) method used in the procured solution, that protects the confidentiality and integrity of the cryptographic keys.

2.10.4.3. Ensure that the procured solution includes the capability for configurable Cryptoperiods (the life span of cryptographic key usage) in accordance with the Suggested Cryptoperiods for Key Types found in Table 1 of NIST 800-57 Part 1.

2.10.4.4. Ensure that the key update method used in the procured solution, supports remote re-keying of all devices within a negotiated period of time as part of normal system operations.

2.10.4.5. Ensure that emergency re-keying of all devices, in the procured solution can be remotely performed within a negotiated period of time (e.g., 30 days).

2.10.4.6. Provide a method for updating cryptographic primitives or algorithms (updates to or replacement of the Cryptographic Method).

2.11. Wireless Technologies

Application Software:

The Supplier shall, where applicable:

2.11.1. Document specific protocols and other detailed information required for wireless device components of the procured product, to communicate.

2.11.2. Document authorized uses, capabilities, and limits for the wireless device components of the procured product.

2.11.3. Document the power and frequency requirements of the wireless device components of the procured product (e.g., microwave devices meet the frequency requirements of Generic Requirements [GR]-63 Network Equipment Building System [NEBS] and GR-1089).

2.11.4. Document the range of the wireless device components of the procured product and verify that the range of communications is minimized to both meet the needs of CPR's proposed deployment and reduce the possibility of signal interception from outside the designated security perimeter.

2.11.5. Outline how the wireless technology and associated devices comply with standard operational and security requirements specified in CPR's wireless security standards and directives.

2.11.6. Demonstrate, through providing summary test data—that known attacks (e.g., those documented in the Common Attack Pattern Enumeration and Classification [CAPEC] list, such as malformed packet injection, man-in-the middle attacks, or denial-of-service attacks) do not cause the receiving wireless devices to crash, hang, be compromised, or otherwise malfunction.

2.11.7. Provide the configuration control options for wireless device components of the procured product.

2.11.8. Provide recommended alarm settings in accordance with the needs of the system.

Integrated Solution, Cloud Solution & ICS:

The Supplier shall:

2.11.9. Document specific protocols and other detailed information required for wireless device components of the procured solution, to communicate.

2.11.10. Ensure that wireless network(s), within the procured solution, are physically and logically segregated from other networks and that access between wireless and wired network goes through an access control device, with an access control policy implemented accordingly.

2.11.11. Document authorized uses, capabilities, and limits for the wireless device components of the procured solution.

2.11.12. Document the power and frequency requirements of the wireless devices in the procured solution (e.g., microwave devices meet the frequency requirements of Generic Requirements [GR]-63 Network Equipment Building System [NEBS] and GR-1089).

2.11.13. Document the range of the wireless devices and verify that the range of communications is minimized to both meet the needs of CPR's proposed deployment and reduce the possibility of signal interception from outside the designated security perimeter.

2.11.14. Document how the wireless technology and associated devices comply with standard operational and security requirements specified in CPR's wireless security standards and directives.

2.11.15. Demonstrate, through providing summary test data—that known attacks (e.g., those documented in the Common Attack Pattern Enumeration and Classification [CAPEC] list, such as malformed packet injection, man-in-the middle attacks, or denial-of- service attacks) do not cause the receiving wireless devices to crash, hang, be compromised, or otherwise malfunction.

2.11.16. Document the configuration control options or wireless device components of the procured solution.

2.11.17. Document recommended alarm settings in accordance with the needs of the system.

2.12. Software Patching

Application Software:

The Supplier shall:

2.12.1. Provide a documented process for acquiring and applying software updates/patches, on an ongoing basis.

2.12.2. Provide a documented process for validating the integrity and traceability of software updates/patches, prior to being applied to the procured product.

Integrated Solution, Cloud Solution & ICS:

The Supplier shall:

2.12.3. Provide a documented process for how software patches can be acquired, distributed and deployed on an ongoing basis, in alignment with CPR enterprise security directives and standards.

2.12.4. Demonstrate that the integrity of the software updates/patches can be determined prior to deployment.

2.12.5. Ensure that the procured product is duly patched, until hand over is completed.

2.13. Backup

Application Software:

The Supplier shall:

2.13.1. Provide a documented process to create and restore a backup of the procured product.

Integrated Solution, Cloud Solution & ICS:

The Supplier shall:

2.13.2. Provide a documented process to create and restore a backup of the procured solution.

2.13.3. Perform the backup, using the documented process and submit a copy to CPR prior to handover.

3. Independent Attestation and Validation/Certification of Cybersecurity Requirements

3.1. Independent Attestation

Application Software:

The Supplier shall:

3.1.1. Provide a third party validation of its information systems, relevant to security, availability, processing integrity, and confidentiality or privacy, or an independent entity-wide assessment of its cybersecurity risk management program (CRMP), by providing the following:

3.1.1.1. SOC 2 Type I report.

3.1.1.2. SOC 2 Type II report.

3.1.1.3. SOC 3 report.

3.1.1.4. International Standard on Assurance Engagements (ISAE) 3402 type II report.

3.1.1.5. Canadian Standard on Assurance Engagements (CSAE) 3416 Type II report.

Integrated & Cloud Solution:

The Supplier shall:

3.1.2. The Supplier shall provide a third party validation of its information systems, relevant to security, availability, processing integrity, and confidentiality or privacy, or an independent entity-wide assessment of its cybersecurity risk management program (CRMP), by providing the following:

3.1.2.1. SOC 2 Type I report.

3.1.2.2. SOC 2 Type II report.

3.1.2.3. SOC 3 report.

3.1.2.4. International Standard on Assurance Engagements (ISAE) 3402 type II report.

3.1.2.5. Canadian Standard on Assurance Engagements (CSAE) 3416 Type II report.

3.2. Validation for ICS Related Products/Services

ICS:

The Supplier shall:

3.2.1. The Supplier shall appoint a CPR-approved independent Third Party Cybersecurity provider, to carry out all required Cybersecurity inspection activities at any location required by CPR, as applicable. This shall include at a minimum:

3.2.1.1. A Factory Acceptance Test (FAT) - Supplier must provide a verification report that validates the security features and functions. In general, prior to initiation of unit testing (as part of FAT), the Supplier shall install the Operating System, application patches, service packs, or other updates certified for use with the system provided at the time of test, and documentation of the configuration baseline. FATs will be witnessed by quality assurance (QA) & technical representatives from the Supplier and CPR personnel, who sign-off and certify that the tests were completed satisfactorily. In the event there is no IFAT (e.g. single system), then the hardening measures on the supplied system happens during the FAT.

3.2.1.2. An Integrated Factory Acceptance Test (iFAT) - Supplier must provide a verification report that validates successful completion of the iFAT. . The first step is to clear the FAT punch lists, before starting the IFAT. The purpose of IFAT is to verify that the centralized security features of multiple systems function properly and provide the expected level of overall functionality. In general, after FAT is conducted on a per system basis, the Supplier shall integrate various other related systems and test their inter-communication interfaces and exchange of secured data among

them accordingly. Satisfactory completion of IFAT, and subsequently providing evidence that all equipment have been checked to be free of malicious code, the Supplier will dispatch the systems to CPR for Site Acceptance Testing(SAT) & Commissioning. Prior to the dispatch, the Supplier will develop and provide "As-built" documents.

3.2.1.3. A Site Acceptance Test (SAT) - The Supplier must provide a verification report that validates successful completion of the SAT. It is expected that SAT be performed in accordance with predefined/approved procedures and acceptance criteria specific to functional requirements as outlined in section 1 to 12. SAT typically repeats FAT to validate that the site installation is equivalent to the systems tested at the factory with additional integrated functions. SAT tests must be witnessed by CPR personnel, who sign-off and certify that the tests are completed satisfactorily and the systems can be accepted by CPR. The SAT will be performed before the cutover or commissioning, and the satisfactory completion of all SAT tests results in commissioning the Supplier delivered systems.

3.2.1.4. A Site Integration Test (SIT) - The Supplier must provide a verification report that validates successful completion of the SIT. SIT must be conducted prior to the hand-over of systems to CPR for operations. Turn-over is the milestone, which completes commissioning and begins the Maintenance & Support phase of the supplied systems' life cycle.

3.2.2. Cybersecurity inspection reports shall be submitted by the Supplier's appointed CPR-approved independent Third Party Cybersecurity Supplier, for each testing phase identified (FAT, iFAT, SAT, SIT) above, and accepted as follows:

3.2.2.1. The approved independent Third Party Cybersecurity Supplier personnel;

3.2.2.2. The Supplier's personnel who witnessed the tests; and

3.2.2.3. The CPR personnel who witnessed the tests.

3.2.3. All Cybersecurity third party inspection reports shall be issued simultaneously to both CPR and the Supplier. At CPRs discretion, CPR may elect to conduct the inspection or testing (e.g. Penetration Testing) alone or in conjunction with a third party Inspection.

3.2.4. All major ICS related equipment and systems shall be subject to Factory Acceptance Tests (FATs). CPR will witness all major Cybersecurity related FATs and SATs.

3.2.5.

3.3. Validation for Procured IT Products/Services

Application Software:

The Supplier shall:

3.3.1. Provide a compliance report, which outlines the procured product's compliance with requirements identified in this schedule.

3.3.2. Provide a non-compliance report, which outlines any exceptions or non-compliance with the requirements identified in this schedule and provide justifications for the non-compliance. The Supplier shall also provide any compensating controls that have been implemented, in lieu of the requirement to which they have not complied.

Integrated & Cloud Solutions:

The Supplier shall:

3.3.3. Provide a compliance report, which outlines the procured solution's compliance with requirements identified in this schedule.

3.3.4. Provide a non-compliance report, which outlines any exceptions or non-compliance with the requirements identified in this schedule and provide justifications for the non-compliance. The Supplier shall also provide any compensating controls that have been implemented, in lieu of the requirement to which they have not complied.

4. Abbreviations & Definitions

4.1. Abbreviations

ACL	Access Control Lists
AES	Advanced Encryption Standard
CAPEC	Common Attack Pattern Enumeration and Classification
CERT	Computer Emergency Response Teams
CSAE	Canadian Standard on Assurance Engagements
CSP	Cloud Service Provider
DSA	Digital Signature Algorithm
FAT	Factory acceptance test
FIPS	Federal Information Processing Standard
GPS	Global Positioning System
GR	Generic Requirements
HIDS	Host Intrusion Detection System
HMI	Human Machine Interface
ICS	Industrial Control System
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronic Engineers
IFAT	Integrated Factory Acceptance Test
ISAE	International Standard on Assurance Engagements
IT	Information Technology
NEBS	Network Equipment Building System
NIDS	Network Intrusion Detection System
NIST	US National Institute of Standards and Technologies
NTP	Network Time Protocol
PLC	Programmable Logic Controllers
RTU	Remote Terminal Unit
SAT	Site Acceptance Test
SCADA	Supervisory Control and Data Acquisition
SDLC	Systems Development Life Cycle
SHA	Secure Hash Algorithm
SIT	Site Integration Test
SOC	Service Organization Control
SSH	Secure Shell Terminal Emulation
TLS	Transport Layer Security
USB	Universal Serial Bus

4.2. Definitions

Access control lists	A list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects
Authentication	A process that allows a device to verify the identity of a subject, connecting to a network resource.
Backdoors	A method, often secret, of bypassing normal authentication or encryption in a computer system, a product, or an embedded device (e.g. a home router), or its embodiment, e.g. as part of a cryptosystem, an algorithm, a chipset
Chain of custody	Chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence.
Cryptographic Algorithm	A procedure or formula for solving a problem, based on conducting a sequence of specified actions.
Cryptographic Key	A piece of information (a parameter) that determines the functional output of a Cryptographic algorithm
Cryptographic Method	The technique used in performing a cryptopgrahic function.
Cryptographic Module	Any combination of hardware, firmware or software that implements cryptographic functions such as encryption, decryption, digital signatures, authentication techniques and random number generation.
Cryptoperiods	Time span during which a specific Cryptographic Key is authorized for use.
Denial of service attack	Any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service.
Encryption	The process of encoding a message or information in such a way that only authorized parties can access it.
Factory acceptance tests (FAT)	These are tests performed in accordance with predefined / approved FAT procedures and acceptance criteria, based on applicable requirements in sections 1 and 2.
Integrated factory acceptance test (iFAT)	Integrated Factory Acceptance Test (iFAT) is performed after successful completion of FAT. It is performed in accordance with an approved procedure, based on applicable requirements in sections 1 and 2
Malware	Any software intentionally designed to cause damage to a computer, server or computer network.
Man in the middle attack	An attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other
Patch	A patch is a set of changes to a computer program or its supporting data designed to update, fix, or improve it.

Protocols	A specific set of communication rules.
Site acceptance test (SAT)	The SAT is a test performed to demonstrate correct implementation of security functions built into a supplied systems.
Site integration test (SIT)	The SIT is a test performed to demonstrate that the factory tested security features on multiple systems function properly as an integrated single system and they provide the expected levels of overall functionality including interfaces with other levels & third party systems
Supplier	An organization or individual that enters into an agreement with the Canadian Pacific Railway Company (CPR) and its affiliates for the supply of IT products or services, including train control system components. This category includes all Suppliers in the supply chain. Supplier also includes any organization that customizes (e.g., combines, adds, or optimizes) components, systems, and corresponding processes. Suppliers may act in a role of integrating components or parts from several other Suppliers.
Systems development lifecycle	This is a framework defining tasks performed at each step in the systems development process. SDLC is a structure followed by a development team within the systems development team or organization
Vulnerabilities	A weakness which can be exploited by a threat actor, such as an attacker, to perform unauthorized actions within a computer system

5. Cybersecurity Requirements Compliance Matrix

Canadian Pacific Railway Company Cybersecurity Requirements Compliance			Compliance/ Agreement (Yes or No)	Comment (Maximum 30 words)
#	**Sections Related to the Applicability Table**			
Supplier's Cybersecurity Program				
1	1.1	Secure Systems Development Practices		
2	1.2	Documentation and Tracking of Vulnerabilities and Notification of Cybersecurity Breaches		
3	1.3	Problem Reporting		
4	1.4	Patch Management and Updates		
5	1.5	Personnel Background Checks		
6	1.6	Secure Hardware and Software Delivery		
Cybersecurity Technical Requirements				
7	2.1.	System Hardening		
8	2.2.	Access Control		
9	2.3.	User Account Management		
10	2.4.	Application Session Management		
11	2.5.	Authentication/Password Policy and Mgmt.		
12	2.6.	Logging and Auditing		
13	2.7.	Communication Restrictions		
14	2.8.	Malware Detection and Protection		
15	2.9.	Intrusion Detection		
16	2.10.	Cryptographic System Management		
17	2.12.	Wireless Technologies		
18	2.13.	Software Patching		
19	2.14.	Backup		
20	2.15.	Software License Management		
Independent Attestation & Validation/Certification of Cybersecurity Requirements				
22	3.1.	Independent Attestation		

Canadian Pacific Railway Company Cybersecurity Requirements Compliance		Compliance/ Agreement (Yes or No)	Comment (Maximum 30 words)
23	3.2. Validation for ICS Related Products/Services		
24	3.3. Validation for IT Procured Products/Services		
	0 - Non-compliant; 1–C ompliant;		

6. Letter to CPR

[Insert CPR Contact Person Full Name]

[Title]

Canadian Pacific Railway Company ("**CPR**")
7550 Ogden Dale Road S.E.
Building #10
Calgary, Alberta, Canada, T2P 4Z4

Dear [Insert Contact Person first name],

We are compliant with the Cybersecurity Requirements checked below. If we are not compliant, we have not checked the box and understand that such response may (at the sole discretion of CPR) eliminate this Proposal from consideration:

☐ **CYBERSECURITY REQUIREMENTS COMPLIANCE MATRIX**
The requirement compliance matrix relating to the Requirements in the Description of Services and/or Materials has been completed and is provided as part of the Proposal

☐ **MANDATORY DOCUMENTATION AS IDENTIFIED IN THE CYBERSECURITY REQUIREMENTS**

Completed the form relating to the Non-Business Requirements

☐ **OTHER FACTORS IDENTIFIED IN YOUR REPLY:**

Best of class services (and offerings) that CPR may not have considered or identified; and, Any restrictions (legal, logistical, etc.) for Supplier to provide these Services in the US or Canada.

☐ **LETTER FROM SUPPLIER TO CPR**
Complete and signed this letter and returned to the CPR Contact Person

Signature: _____ Name: _

Title: _____ Company: _____

Date: _____

Revision History

Version	Author	Date	Description
Initial Draft	Darcy MC	Sept 27, 2018	First draft.
Final Draft	Tony Arthur	Dec 10, 2018	Updated content based on ES review meeting.
1.3	Tony Arthur	Jan 23, 2019	Updated content based on feedback from CSS.
1.5	Tony Arthur	Jan 28, 2019	Final doc.

Approval

Approved by: Tony Arthur
Director, Enterprise Security

Date