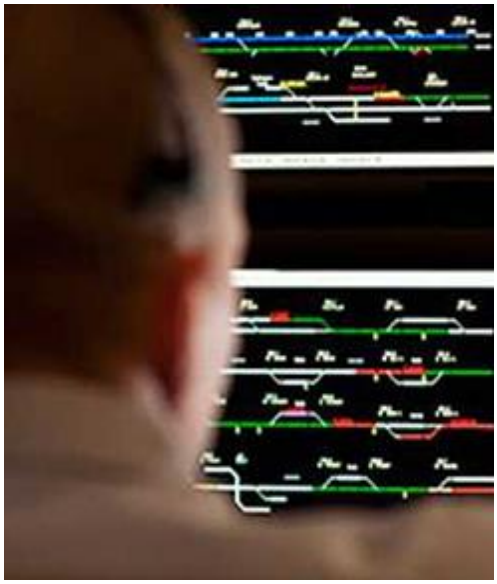
ASSOCIATION OF AMERICAN RAILROADS (AAR)

Rail Information Security Committee

Cyber Security Effective Practices for Information Technology Procurements



For Questions or Comments

Rail sector asset owners, operators, and suppliers are encouraged to provide feedback on this document. Please send questions, comments, or suggested enhancements to RailwayAlertNetwork@aar.org.

Acknowledgements

This document was adapted by the Rail Information Security Committee (RISC) from a product produced, in part, by the Electricity Sector Control Systems Working Group (ESCSWG) entitled Cy*bersecurity Procurement Language for Energy Delivery Systems*. Sincere appreciation is extended to that group for agreeing to the adaptation of its 2014 product.

Disclaimer

Contents

1. INTRODUCTION

1.1 Cybersecurity of Railroad Systems

The business and technology environments for the North American railroad industry are evolving at a healthy pace. In modern railroads, core business processes are largely and increasingly reliant on information technologies (IT) that underpin, and are integrated with, railroad operations. As railroads leverage more technology, and as that technology is more closely tied to operations, both the opportunity for cyber-attacks and the potential consequences of a successful attack may increase. At the same time, the Nation as a whole, and private sector industries generally, including railroads, face cyber threats intensifying in scope, complexity, and potential effects. Absent sustained, proactive efforts in risk mitigation, these trends have the opportunity to drive increasing cyber risk for railroads.

As an industry over 150 years old, railroads understand the critical importance of offering secure business solutions. Across the industry, companies invest in high-quality capabilities to protect the integrity of sensitive systems and networks and the information that enhances their operations. To amplify its reach, the industry coordinates and establishes partnerships that deliver timely and actionable cyber intelligence and benchmarks its security posture against internationally recognized standards and effective practices to stay in front of emerging threats. The rail industry has taken, and will continue to take, necessary actions to mitigate cyber risk.

Central to efforts to elevate the capabilities of the nation's railroads to mitigate cyber risk and counter cyber threats, the industry formed the Rail Information Security Committee (RISC) in 1999. The RISC is comprised of the chief information security officers and cyber security leads from each of the Class I railroads, Amtrak, Genesee and Wyoming, VIA Rail, and Railinc, supported by the Association of American Railroads (AAR). The objectives of the group are to: 1) improve and maintain the overall information security of each road and the industry; and 2) coordinate incident response analysis and recommendations.

The group regularly convenes to develop and share effective practices and threat, vulnerability, and incident response information, including:

- Industry-wide information sharing through the Railway Alert Network (RAN) at AAR.
- Information sharing with government departments and agencies in the United States and Canada with responsibilities relating to cyber security.
- Coordinated responses to governmental inquiries related to industry information security practices.

- Security benchmarking activities against well established and proven cybersecurity standards and recognized effective practices.
- Periodic review and comparative analysis of activities and key projects.
- Annual assessments of each railroad's information assurance programs against industry-accepted and internationally-recognized standards.
- Consultations on effectiveness of cyber security strategies and protective measures.
- Sharing of experience with and information on effective cyber security practices, tools, and resources.
- Security specifications are evaluated for industry development initiatives

Looking forward, railroads can expect to encounter robust cyber threats and will need to continue to evolve security programs, considering a dynamic risk environment and the potential for increasing use of technology for safe and more efficient operations.

1.2 The Role of Suppliers Impacting the Cybersecurity of Rail Systems

Systems that support the full range of complex business processes involved in running a railroad may include IT solutions or IT components that are acquired or integrated from Suppliers. These solutions often are integral to back-office data processing and/or integrated with operational technologies that may closely link with transportation operations. Because of the dynamic nature of cyber threats, the scale of IT integration and interoperability, and the key role that Suppliers play in the delivery of solutions for railroads, the RISC has developed this compilation of effective practices as an industry resource to inform consultations with Suppliers of railroad technologies.

This compilation may be shared with organizations that design, develop, integrate and supply IT systems in support of railroads.

These effective practices complement existing cybersecurity efforts by outlining expectations of capabilities and measures in a clear manner. Desired outcomes include:

Ensure resiliency: Design, install, operate, and maintain railroad systems that will survive a cyber incident while sustaining critical functionality.

Improve engagement: Proactive integration of cybersecurity expectations in interactions with Suppliers supports a culture of security, helping to bolster protective measures and inform productive interaction between Suppliers and Acquirers on important cybersecurity concerns.

Improve security: Consideration of cybersecurity and of potential vulnerabilities in the supply chain of information technology systems and components in procurements are elements of a mature security capability. It is the expectation of the participating railroads that Suppliers will apply the practices delineated in this document to deliver products, capabilities, and services that address cyber risk.

Reduce supplier risk: By utilizing identified and consolidated effective practices to inform procurement decisions, railroads can reduce risks associated with the acquisition and integration of information technology and industrial control systems.

1.3 How to Use this Document

Key Definitions

Key terms used throughout this document describe the two broad categories of users, the "Acquirer" (e.g., purchaser or buyer) and the "Supplier" (e.g., vendor, seller, integrator, or manufacturer).

- Acquirer: Stakeholder that acquires or procures a product or service.
- Supplier: Organization or individual that enters into an agreement with the Acquirer for supplying a product or service. 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.

This document provides baseline cybersecurity effective practices that have been reviewed and approved by the RISC. This document should be used to supplement an organization's existing IT management processes and standards, as a means of reducing the risk that procurement and use of a Supplier's products will exacerbate cybersecurity risk for the Acquirer. Acquirers may use this document to guide engagement and procurement practices when working with Suppliers, to reduce the risk that the Supplier's products will present major cybersecurity challenges for the Acquirer. Acquirers may refer to this document when making procurement decisions or when negotiating with Suppliers.

Suppliers may use this document as a guide to align their practices with the reasonable expectations for cybersecurity of railroad Acquirers.

Categories of cybersecurity effective practices addressed in this compilation are:

- Individual components of railroad systems (e.g., programmable logic controllers, digital relays, or remote terminal units).
- Individual railroad systems (e.g., a SCADA system, ICS, or Control Systems).
- Assembled or networked railroad systems (e.g. back office or operational systems, for example on locomotives or wayside installations).
- Suppliers of services for railroad systems (e.g., consulting, support and maintenance activities).

Specifically, this document may be used for the following purposes:

- Acquirers seeking to incorporate cybersecurity into the procurement of railroad systems or components. Relevant specifications may be issued by the Acquirer through requests for proposal (RFPs) or requests for information (RFIs).
- Acquirers seeking to evaluate the cybersecurity maturity of railroad systems or components offered by Suppliers.
- Suppliers designing or manufacturing systems, components, and services that align with cybersecurity features sought by Acquirers.
- Acquirers and Suppliers negotiating procurement contracts that outline cybersecurity features and responsibilities for each party involved in the procurement.
- Acquirers and Suppliers currently engaged with railroads in support of existing railroad systems or otherwise providing services related to railroad systems.
- Suppliers may use this document to communicate to internal stakeholders the expectations of the Acquirer with regard to cybersecurity.

Unless otherwise specified, the procurement language in this document applies “at the point of delivery” of the product.

When a railroad system contains components from multiple Suppliers, additional cybersecurity procurement language may be required to ensure the secure delivery and integration of those components.

2. EFFECTIVE PRACTICES FOR SUPPLIERS – GENERAL

This section presents cybersecurity effective practices for railroad systems that may be applicable to a single component of a system, a complete system, or a set of integrated systems.

2.1 Software and Services

Unused and unnecessary software and services in railroad systems and components that are left enabled can pose potential entry points for exploits, especially if they are not monitored. These services can range from system diagnostics to chat programs. Various attacks have been crafted to exploit these vulnerabilities, leading to the compromise. These vulnerabilities can be addressed by the "principle of least functionality," which states that programs or processes must only be able to access the information and computational resources that are needed for them to perform their intended function.

Primary effective practices:

2.1.1. Remove all software components that are not required for the operation and/or maintenance of the procured product. If removal is not technically feasible, then the Supplier shall disable software not required for the operation and/or maintenance of the procured product. This removal shall not impede the primary function of the procured product. If software that is not required cannot be removed or disabled, the Supplier shall document a specific explanation and provide risk mitigating recommendations and/or specific technical justification. The Supplier shall provide documentation on what is removed and/or disabled. The software to be removed and/or disabled shall include, but not be limited to:

- Games
- Device drivers for product components not procured/delivered
- Messaging services (e.g., email, instant messenger, peer-to-peer file sharing)
- Source code
- Software compilers in user workstations and servers
- Software compilers for programming languages that are not used in the railroad system
- Unused networking and communications protocols

- Unused administrative utilities, diagnostics, network management, and system management functions
- Backups of files, databases, and programs used only during system development
- 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. Remove and/or disable, 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., 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. Configure the procured product to allow the Acquirer the ability to re-enable ports and/or services if they are disabled by software.

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

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

2.2 Access Control

Products that do not have appropriate access control methods in place can allow adversaries to gain unauthorized or undetected access to systems. Access control is the process of restricting access to certain systems, information, functions, tools, locations, components, or resources. Access control limits individual users and processes by implementing the "principle of least privilege" so that every process, program, or user shall only access the information and resources for which it is authorized and that are necessary for operation. This measure reduces the number of potential entry points for an attack. Access control is designed to enforce security policies and streamline security management processes by grouping users based on their role within the organization, rather than separately evaluating each individual identity.

Primary effective practices:

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. 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.

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

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

2.2.5. Recommend methods for the Acquirer 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. Verify and provide documentation for the procured product, attesting that unauthorized logging devices are not installed (e.g., key loggers, cameras, and microphones), as specified by the Acquirer.

Secondary effective practices:

2.2.7. Configure the procured product such that when a session or inter-process communication is initiated from a less privileged application, access shall be limited and enforced at the more critical side.

2.2.8. Deliver a product that enables the ability for the Acquirer 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 documentation of the product's configuration as delivered.

2.3 Account Management

Many railroad systems are configured with default accounts and passwords that are sometimes publicly available. In some cases, these accounts can be used to gain unauthorized system access or to escalate privileges.

Primary effective practices:

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

2.3.2. Change default account settings to Acquirer-specific settings (e.g., length, complexity, history, and configurations) or support the Acquirer in these changes. The Supplier shall not publish changed account information. The Supplier shall provide new account information to the Acquirer via a protected mechanism.

2.3.3. Prior to delivery of the procured product, remove, or disable any accounts that are not needed for normal or maintenance operations of the railroad system.

2.3.4. As specified by the Acquirer, place accounts for emergency operations in a highly secure configuration, with documentation on their configuration provided to the Acquirer.

2.4 Session Management

Weak or insecure system session operating practices can result in vulnerabilities in railroad systems. Examples of insecure practices include permitting use of clear text passwords, passwords lacking requisite complexity, multiple concurrent session logins, remembered account information between logins, and auto-filling fields during logins. Once an account is compromised, system administrators have no way of knowing with certainty whether the account is being used by an unauthorized party.

Primary effective practices:

2.4.1. Preclude user credentials from being transmitted or shared in clear text. Do not store user credentials in clear text, unless the Supplier and Acquirer agree that this is an acceptable practice for the procured product given the protection offered by other security controls. Only allow 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. Provide an appropriate level of protection (e.g., encryption and digital signing) for the session, as specified by the Acquirer, commensurate with the technology platform, communications characteristics, and response time constraints.

2.4.3. Unless specifically requested by the Acquirer, do not allow multiple concurrent logins using the same authentication credentials, allow applications to retain login information between sessions, provide any auto-fill functionality during login, or allow anonymous logins.

2.4.4. 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

The need for constant availability of railroad systems often results in weak password policies, which can provide easy entry points into railroad systems. This may be caused by users selecting poor or easily guessed passwords that attackers can break within minutes.

Primary effective practices:

2.5.1. Document the levels, methods, and capabilities for authentication and authorization. Deliver a product that adheres to standard authentication protocols.

2.5.2. Protect passwords, including not storing passwords in clear text and not hardcoding passwords into software or scripts.

2.5.3. If needed for ongoing support and maintenance, the Supplier's solutions involving interactive remote access/control shall adhere to (i.e., be compatible with) the Acquirer's implementation of multifactor authentication (e.g., two-factor or token).

Secondary effective practices:

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

- Changes to passwords (including default passwords)
- Selection of password length
- Frequency of change
- Setting of required password complexity
- Number of login attempts prior to lockout
- Inactive session logout
- Screen lock by application
- Comparison to a library of forbidden strings
- Derivative use of the user name
- Denial of repeated or recycled use of the same password

2.5.5. Provide a centralized and local account management capability.

Primary effective practices for secure single sign-on:

2.5.6. Ensure that account access for single sign-on is equivalent to that enforced as a result of direct login.

2.5.7. Use a secure method of authentication (e.g., strong two-factor authentication) to allow single sign-on to a suite of applications.

2.5.8. Protect key files and access control lists used by the single-sign-on system from non-administrative user read, write, and delete access. The single sign-on system must resolve each individual user's credentials, roles, and authorizations to each application.

2.5.9. Provide documentation on configuring a single-sign-on system, as well as documentation showing equivalent results in running validation tests against the direct login and the single sign-on.

2.6 Logging and Auditing

Recording specific system activity in the form of logging generates an audit trail. Failure to perform logging makes it difficult to monitor activity, identify potential cyberattacks in time to take protective actions, perform diagnostics, and carry out forensic activities in the event of a successful cyberattack. Without easy access to information on system activity, post-event investigations may not yield conclusive results and the risk of similar events occurring in the future would remain high.

Primary effective practices:

2.6.1. Provide logging capabilities or the ability to support the Acquirer's existing logging system. Logging capabilities shall be configurable by the Acquirer and support the Acquirer's security auditing requirements. As specified by the Acquirer, 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. Provide standard time synchronization in the procured product (e.g., Global Positioning System [GPS], Network Time Protocol [NTP], and Institute of Electrical and Electronic Engineers [IEEE] Standard 1508-2008). If the Supplier is not providing standard time synchronization but is providing an authoritative time source, the procured product shall be configured to synchronize to the authoritative time source.

2.6.3. Time stamp audit trails and log files, as specified by the Acquirer.

2.6.4. If required by the Acquirer, provide confidentiality and integrity security protection of log files.

2.6.5. Implement an approach for collecting and storing (e.g., transfer or log forwarding) security log files.

2.6.6. Provide a list of all log management capabilities that the procured product is capable of generating and the format of those logs. This list shall identify which of those logs are enabled by default.

Secondary effective practices:

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

2.7 Communication Restrictions

Poorly designed network architectures that lack a defense-in-depth approach to security may be vulnerable to cyber exploitation. Security can be enhanced by partitioning networks into multiple segments and placing technical security controls (e.g., firewalls, unidirectional communication devices, or virtual private network [VPN] concentrators) between the network segments. Hardware, software, and firmware that restrict communications are important tools in establishing an appropriate cybersecurity defensive architecture. The network architecture is how a network is designed and segmented into logical, smaller functional subnets (i.e., network security zones) for the purpose of communication.

Primary effective practices for the acquisition of networked railroad systems:

2.7.1. Function in a zoned environment specified by the acquirer permitting restriction of communications between the product components and external systems. Document ports and protocols in use and methods for isolating the system while continuing limited operations. Provide information on all communications required between network security zones, identify each network component of the procured product initiating communication, and provide a method to restrict communication traffic between different network security zones. Provide documentation on any method or equipment used to restrict communication traffic and shall document that disconnection points are established between network security zones.

2.7.2. If firewalls are provided, deliver documentation on the firewalls and their firewall rule sets for normal and emergency operations. If the Acquirer 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.

2.7.3. Document all remote access entry pathways and ensure that they can be enabled or disabled by the Acquirer as needed.

Secondary effective practices for the acquisition of networked railroad systems:

2.7.4. 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.

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

2.7.6. Verify that the procured product allows 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 the Acquirer's network. Where this is not available, the Supplier shall offer an alternative approach, with mitigating security measures, that is acceptable to the Acquirer.

Secondary effective practices for products that utilize communication tunneling (e.g., using a VPN):

2.7.7. Provide or utilize an existing security-isolated environment 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.

2.7.8. Employ different authentication credentials from those used for in-network communications when establishing control network access using communication tunneling.

2.7.9. 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. This measure shall address confidentiality and/or integrity, as specified by the Acquirer.

Secondary effective practices for the acquisition of railroad system networks or networking components:

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

2.7.11. Verify and provide documentation that the network configuration management interface is secured.

2.7.12. Provide 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

Malicious code (e.g., malware) comes in many shapes and forms. Most often it is spread in the form of Trojans and viruses by users of personal computers, laptops, and other devices via USB connections, email messages with attached malicious files, or access to websites – by clicking links – infected with malicious software. Malicious code can enter systems through removable media. It can also be self-propagating in the form of worms. As railroad systems migrate onto Internet Protocol (IP)-based platforms, they become more susceptible to malware infections and require cyber protections against them.

Secondary effective practices for the acquisition of railroad systems and components with malware protection capabilities:

2.8.1. Provide, or specify how to implement, the capability to scan automatically any removable media that is introduced to the product being acquired.

2.8.2. Implement at least one of the following:

- Provide a host-based malware detection capability. 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.
- If the Supplier is not providing 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.
- If the Supplier is not providing a host-based malware detection capability, nor suggesting malware detection products, and if specified

by the Acquirer, the Supplier shall provide an application whitelisting solution that is tested, validated, and documented that shall only permit approved applications to run.

2.8.3. Validate that cybersecurity services running on the procured product (e.g., virus checking and malware detection) do not conflict with other such services running on the procured product.

2.9 Heartbeat Signals

Heartbeat signals are the regularly repeated signals generated by hardware, software, or firmware to indicate normal operation or for synchronization with other components within a railroad system. Heartbeat signals can be configured in the hardware, software, or firmware. If a heartbeat signal is not received in the prescribed time, it is an indication that the component generating the signal is not operating within its normal parameters. Heartbeat signals can be sent over serial connections or routed protocols. Problems may arise when heartbeat signals or protocols are corrupted, spoofed, or possibly used as an entry point for unauthorized access.

Secondary effective practices:

2.9.1. Identify heartbeat signals or protocols and recommend which should be included in network monitoring. At a minimum, a last gasp report from a dying component or equivalent shall be included in network monitoring.

2.9.2. Provide packet definitions of the heartbeat signals and examples of the heartbeat traffic if the signals are included in network monitoring.

2.10 Reliability and Adherence to Standards

Adherence to security standards is one step in protecting railroad systems and components from compromise. These standards should be considered when procuring railroad systems and components in order to improve security implementation, including the protection of sensitive information.

Primary effective practices:

2.10.1. Protect the confidentiality and integrity of the Acquirer's sensitive information.

2.10.2. Verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput specified.

2.10.3. Use an implementation that complies with the current applicable interoperability and security standards, as specified by the Acquirer (e.g., NIST 800 series, ISA/IEC 62443, IEEE 1613, IEEE 1588, and NERC CIP).

2.10.4. Upon the Acquirer's request, return or document the secure disposal of the Acquirer's data and Acquirer-owned hardware that is no longer needed by the Supplier (e.g., NIST Special Publication [SP] 800-80).

3. THE SUPPLIER'S LIFE CYCLE SECURITY PROGRAM

The life cycle security program is an important consideration in the procurement process. System and network vulnerabilities frequently result from architecture or design, weaknesses and from vulnerabilities in hardware, software, and firmware coding, as well as in bundled third-party products. Many railroad system security vulnerabilities are the direct result of writing of the software with inadequate attention to secure coding practices that reduce the risk of successful deliberate and persistent malicious attacks. Life cycle security programs provide a structured way for developing robust products with fewer weaknesses and vulnerabilities or finding and remediating them before software and systems are delivered and installed in the Acquirer's environment. Supplier post-production support is critical for maintaining secure software and systems, including remediating newly discovered vulnerabilities and ensuring that spare parts can be replaced with genuine parts. Validating that hardware, software, or firmware has been delivered as it was ordered and shipped – without being tampered with or otherwise modified – is also important. After a product has been removed from service, the disposal of that product provides opportunities for the compromise of information and configurations that the Acquirer or Supplier may deem sensitive.

3.1 Secure Development Practices

Secure product development practices are a set of processes integrated into the system development life cycle (SDLC) that reduce the security risks of the overall product. These practices help to develop more robust hardware, software, and firmware with fewer

weaknesses and vulnerabilities, as well as identify and remediate weaknesses and vulnerabilities before implementation. Secure development practices ensure that security is integrated into all phases of the SDLC and is considered a key component of system development.

Baseline effective practices:

3.1.1. Provide summary documentation of the secure product development life cycle including the standards, practices (including continuous improvement), and development environment (including the use of secure coding practices) used to create or modify Supplier-provided railroad system hardware, software, and firmware. If applicable, document how the most critical application security weaknesses (including *OWASP Top 10* or *SANS Top 25 Most Dangerous Software Errors*) are addressed in the SDLC.

3.1.2. As specified by the Acquirer, identify the country (or countries) of origin of the procured product and its components (including hardware, software, and firmware). Identify the countries where the development, manufacturing, maintenance, and service for the product are provided. Notify the Acquirer of changes in the list of countries where product maintenance or other services are provided in support of the procured product. This notification shall occur within [a negotiated time period] prior to initiating a change in the list of countries.

3.1.3. Provide a Quality Assurance program and validate that the software and firmware of the procured product have undergone Quality Control testing to identify and correct potential cybersecurity weaknesses and vulnerabilities. This testing shall include fuzz testing, static testing, dynamic testing, and penetration testing. Use positive and appropriate negative tests to verify that the procured product operates in accordance with requirements and without extra functionality, as well as monitor for unexpected or undesirable behavior during these tests. This testing may be done by the Supplier or an independent entity. Provide summary documentation of the results of the testing that includes unresolved vulnerabilities and recommended mitigation measures.

3.1.4. Provide summary documentation of its coding reviews, including defect lists and plans to correct identified vulnerabilities.

3.1.5. Communicate security-related technical issues with a single technical point of contact (e.g., a company support email address or a company support phone number), as specified by the Acquirer. Communicate with the Acquirer within [a negotiated time period] (see Section 3.3.3). This is not intended for non-technical contract-related issues.

3.1.6. Provide documentation of all input validation testing including, but not limited to, measures for prevention of command injection, Structured Query Language (SQL) injection, directory traversal, Remote File Include, Cross-Site Scripting (XSS), and buffer overflow.

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

3.1.8. The Acquirer shall have the right to request documentation of the Supplier's implemented cybersecurity program, including recent assessment results or conduct periodic [at a negotiated frequency and scope] on-site security assessments at the Supplier's facilities. These on-site security assessments may be conducted by an independent third party, at the discretion of the Acquirer.

3.2 Documentation and Tracking of Vulnerabilities

When security vulnerabilities are discovered in hardware, software, and firmware, the timely application of corrective actions and/or mitigation steps can reduce the likelihood that adversaries will be able to exploit these vulnerabilities in railroad systems. Some of these vulnerabilities may be publicly disclosed before the Supplier can develop remedies; others may be kept from disclosure until remedies are available.

Security breaches may also affect the cybersecurity of the procured product. Such breaches may involve a compromise of security involving the Supplier's organization, or any organization involved in the product's supply chain. Security breaches may result in the loss of sensitive product design information, information on the Acquirer's use and configuration of the product, a compromise of access control information for the deployed products (e.g., compromise of access control information that the Supplier uses to perform maintenance on

a deployed product), or other security-sensitive information. If the Acquirer is informed of a security breach in a timely manner, it may be able to apply mitigating measures to maintain adequate levels of security.

Baseline effective practices:

3.2.1. Upon request of the Acquirer, and prior to the delivery of the procured product, provide summary documentation of publicly disclosed vulnerabilities in the procured product and the status of disposition of those publicly disclosed vulnerabilities.

3.2.2. Provide, within [a negotiated time period] after product delivery, summary documentation of uncorrected security vulnerabilities in the procured product. This summary includes information on vulnerabilities that have not been publicly disclosed or have only been identified after the delivery of the product. The summary 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.

3.2.3. After contract award, provide summary documentation within [a negotiated time period] of any identified security breaches involving the procured product 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 product.

3.3 Problem Reporting

It is difficult to build products that are perfectly secure, and sometimes unknown vulnerabilities exist in the core logic and configuration of railroad systems and components. When vulnerabilities in hardware, software, or firmware configurations are discovered by users, a process is needed to allow users to report them. 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.

Baseline effective practices:

3.3.1. Provide a secure process for users to submit problem reports and remediation requests. This process shall include tracking history and corrective action status reporting.

3.3.2. Provide the Acquirer with its responsible disclosure and threat reporting policies and procedures (e.g., Computer Emergency Response Teams [CERTs]), which shall address public disclosure protections implemented by the Supplier.

3.3.3. Upon the Acquirer submitting a problem report, the Supplier shall review the report, develop an initial action plan within [a negotiated time period], and provide status reports of the problem resolution to the Acquirer within [a negotiated time period].

3.4 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 Suppliers 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.

Baseline effective practices:

3.4.1. Provide documentation of the applicable patch management program and update process (including third-party hardware, software, and firmware). This documentation shall include resources and technical capabilities to sustain this program and process. This includes the Supplier's method or recommendation for how the integrity of the patch is validated by the Acquirer. This documentation shall also include the Supplier's approach and capability to remediate newly reported zero-day vulnerabilities.

3.4.2. Verify and provide documentation that procured products (including third-party hardware, software, firmware, and services) have appropriate updates and patches installed prior to delivery to the Acquirer, or within [a pre-negotiated period] after delivery.

3.4.3. For [a negotiated time period of the contract or support agreement], the Supplier shall provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses within [a negotiated time period]. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, within [a negotiated time period (e.g., 7, 14, or 21 days)]. If updates cannot be made available by the Supplier within these time periods, the Supplier shall provide mitigations and/or workarounds within [a negotiated time period].

3.4.4. When third-party hardware, software, and firmware is provided by the Supplier to the Acquirer, the Supplier shall provide appropriate hardware, software, and firmware updates to remediate newly discovered vulnerabilities or weaknesses within [a negotiated time period]. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, within [a negotiated time period (e.g., 30, 60, or 90 days)]. If these third-party updates cannot be made available by the Supplier within these time periods, the Supplier shall provide mitigations and/or workarounds within [a negotiated time period].

3.5 Supplier Personnel Management

Supplier personnel who have access to an Acquirer's railroad system, or have sensitive information about the system, need to protect this information from adversaries. Without Supplier personnel management processes, sensitive information and access to assets could be compromised when changes to a Supplier's staff occur.

Baseline effective practices for railroad systems:

3.5.1. Provide summary documentation to attest to its workforce receiving position-appropriate cybersecurity training and awareness. This element includes specialized training for those involved in the design, development, manufacture, testing, shipping, installation, operation, and maintenance of products procured by the Acquirer, as part of the Supplier's cybersecurity program.

3.5.2. Perform security background checks on its employees (including contract personnel) working directly on or involved in the development of an Acquirer's system or procured product. The background check methodology shall be

mutually agreed upon by the Acquirer and Supplier.

3.5.3. Ensure that policies and procedures are followed to prohibit the unauthorized disclosure of knowledge, information, architectures, or configuration relevant to the Acquirer's system.

3.5.4. Share information to support the timely update of authentication credentials and access control to reflect staffing changes.

3.6 Secure Hardware and Software Delivery

Railroad systems use information and communication technology (ICT). The modern ICT supply chain is complex and extended, and it provides numerous opportunities for subversion, including malicious code insertion, counterfeit insertion, and tampering. Specifically, ICT, including railroad systems, requires protection during delivery, both physical (when components are transported) and logical (when software, including patches, is downloaded). If railroad systems and their components are not protected during delivery, the resulting production systems may fail prematurely or exhibit unintended functionality, which can compromise railroad system availability, reliability, and integrity.

Baseline effective practices:

3.6.1. Establish, document, and implement risk management practices for ICT supply chain delivery of hardware, software, and firmware. Provide documentation on its:

- Chain-of-custody practices
- Inventory management program (including the location and protection of spare parts)
- Information protection practices
- Integrity management program for components provided by sub-suppliers
- Instructions on how to request replacement parts
- Maintenance commitment to ensure that for a specified time into the future, spare parts shall be made available by the Supplier

3.6.2. Specify how digital delivery for procured products (e.g., software and data) will be validated and monitored to ensure the digital delivery remains as specified. If the Acquirer deems that it is warranted, the Supplier shall apply encryption to protect procured products throughout the delivery process.

3.6.3. Use trusted channels to ship critical railroad system hardware, such as U.S. registered mail.

3.6.4. Demonstrate a capability for detecting unauthorized access throughout the delivery process.

3.6.5. Demonstrate chain-of-custody documentation for critical railroad system hardware and require tamper-evident packaging for the delivery of this hardware.

4. INTRUSION DETECTION

Intrusion detection is used to detect attempts to compromise the confidentiality, integrity, or availability of railroad systems. An intrusion detection system (IDS) is a component, or specialized software residing on a component, that monitors network or system activities for malicious activities or policy violations and logs or reports potential issues. Intrusion detection on railroad systems can involve the use of host-based or network-based IDSs.

4.1 Host Intrusion Detection

A host-based intrusion detection system (HIDS) is one of the last layers of protection for the systems on a network. HIDS is used to monitor and analyze the communication traffic within a system component or railroad system. It can also be used to assess communication traffic at the component's network interfaces. The HIDS monitors and reports the configuration of the host system and application activity. HIDS may perform such functions as log analysis, event correlation, integrity checking, policy enforcement, rootkit detection, performance monitoring, and base-lining to detect variations in system configuration.

Baseline effective practices for the acquisition of a component or railroad system with HIDS:

4.1.1. Provide either a configured HIDS or the information needed for the Acquirer to configure the HIDS.

4.1.2. Implement or recommend a configuration for the HIDS in a manner that adheres to requirements for the Acquirer's operating system functions or business objectives.

4.1.3. Apply the auditing and logging provisions outlined in Section 2.6 of this document to the HIDS.

4.2 Network Intrusion Detection

A network intrusion detection system (NIDS) is used to identify and analyze communication traffic on a computer network and to identify unauthorized or malicious activity. NIDS can be either knowledge-based or behavior-based. Due to the nature of monitoring, NIDS generates voluminous logs. If these logs are not properly configured during initial setup, they may become unmanageable, and therefore not useful. Performing the initial configuration of the NIDS is a minor effort compared to the degree of effort required for ongoing log reviews and tuning. Log consolidation, review, and notification software tools should be used to help automate the review of NIDS data.

Baseline effective practices for the acquisition of a component or railroad system with a NIDS:

4.2.1. Recommend placement(s) of the NIDS sensors to provide appropriate monitoring for the railroad system network.

4.2.2. Provide traffic profiles with expected communication paths, network traffic, and expected utilization boundaries for behavior-based (also called anomaly based) NIDS.

4.2.3. Provide initial and routinely updated signatures for knowledge-based (also called signature-based) NIDS.

4.2.4. Provide either a configured NIDS or the information needed for the Acquirer to configure the NIDS in adherence to the Acquirer's functional requirements.

4.2.5. Provide a NIDS architecture that works with the system communication method.

5. PHYSICAL SECURITY

Physical security is an important element in cyber defense for railroad systems. Physical security is used to deter, delay, detect, and deny physical access by unauthorized individuals, including those who may wish to physically access railroad system components in order to compromise the confidentiality, integrity, or availability of the systems or their data. The Acquirer can insert appropriate physical security requests in its effective practices for railroad systems.

5.1 Physical Access to Railroad System Components

Physical security is a key aspect of protecting railroad systems from manipulation, sabotage, or theft. The innermost level of physical security involves deterring and delaying an adversary from gaining access to the railroad system or its components once inside the facility.

Baseline effective practices for the acquisition of new railroad systems, when the Acquirer does not have existing physical security enclosures and wishes to include them:

5.1.1. Provide lockable or locking enclosures or rooms for railroad systems and system components (e.g., servers, clients, and networking hardware) and for the systems used to manage and control physical access (e.g., servers, lock controllers, and alarm control panels).

5.1.2. Provide a method for tamper detection on lockable or locking enclosures. If a physical security and monitoring system is used, tamper detection shall be compatible.

5.1.3. Change locks, locking codes, keycards, and any other keyed entrances within [a pre-negotiated period] or provide the tools and instructions for making these changes.

5.1.4. Consult and coordinate with Acquirer to verify that physical security features do not hamper railroad system operations.

5.1.5. Reprogram codes (e.g., remove default codes) on provided locks and locking devices so that the codes/passwords are unique to the Acquirer and do not repeat codes used in the past.

5.1.6. As specified by the Acquirer, provide two-factor authentication for physical access control.

5.2 Perimeter Access

Perimeter security is one of the first lines of defense for protecting a facility and its internal systems. A breach of this perimeter can lead to the compromise of railroad systems. Perimeter security components that restrict physical access to a facility or a portion of a facility include fences, walls, entrance gates or doors, vehicle barriers, surveillance and alarm systems, and security guards. Perimeter access restrictions are used to prevent unauthorized individuals from entering areas where railroad systems and their communication pathways are located.

Baseline effective practices for the acquisition of a physical perimeter access system:

5.2.1. Provide a physical security assessment as specified by the Acquirer and relevant to the procurement that defines the security perimeter physical access points and controls needed at each access point.

5.2.2. Coordinate with local authorities when installing and using remote alarm systems, as defined and specified by the Acquirer.

5.2.3. Verify and provide documentation that monitoring and alarm of physical access can be separated from the control network (unless making this communication part of the control network is specifically requested by the Acquirer).

Baseline effective practices when the Supplier is also involved in the operation of the physical perimeter access system:

5.2.4. Allow access within the perimeter only to those employees, contractors, or guests explicitly permitted in such access by both the Supplier and Acquirer.

5.2.5. Verify and provide documentation that security personnel have completed background checks.

5.3 Communications inside the Physical Security Perimeter

Compromise of the communications within a security perimeter can jeopardize the security of railroad systems. These communications need to be secured to limit access to railroad systems and their data, which should flow to only authorized users. These communications may involve wired or wireless systems.

Baseline effective practices for the acquisition of communications that are internal to the Acquirer's system:

5.3.1. Verify and provide documentation that physical communication channels are secured from physical intrusion.

5.3.2. Verify and provide documentation that communication channels are as direct as possible (e.g., communication paths between devices in the same network security zone do not pass through devices maintained at a lower security level or unnecessarily cross into zones of lower physical security).

6. WIRELESS TECHNOLOGIES

Wireless technologies refer to any technology (e.g., radio, microwave, infrared, and ZigBee) that allows analog and digital communication without the use of wires.

6.1. General Wireless Technology Provisions

Many railroad systems and networks use wireless technologies; therefore, it is important to establish and maintain effective and reliable wireless communications links. Unlike wired networks, access to wireless networks does not require physical access or the typical permissions associated with physical access. It is important to utilize sufficient security protections to mitigate the threat of the wireless network being used by individuals without the organization's knowledge or consent.

Baseline effective practices for wireless technology:

6.1.1. Document specific protocols and other detailed information required for wireless devices to communicate with the control network, including other wireless equipment that can communicate with the Supplier-supplied devices.

6.1.2. Document authorized uses, capabilities, and limits for the wireless devices.

6.1.3. The Supplier shall document the power and frequency requirements of the wireless devices (e.g., microwave devices meet the frequency requirements of Generic Requirements [GR]-63 Network Equipment Building System [NEBS] and GR-1089).

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

6.1.5. Document that the wireless technology and associated devices comply with standard operational and security requirements specified in applicable wireless standard(s) or specification(s) (e.g., applicable IEEE standards, such as 802.11).

6.1.6. 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.

6.1.7. Document the configuration control options that enable varying of the security level of the devices.

6.1.8. Allow and recommend alarm settings in accordance with the needs of the system.

7. CRYPTOGRAPHIC SYSTEM MANAGEMENT

A cryptographic-based security system involves both cryptographic methods (e.g., primitives/algorithms) and Cryptographic Key Management (CKM) (methods of creating, distributing, maintaining, validating, and updating cryptographic keys). This document addresses basic cryptographic system documentation and management capabilities that are to be provided.

This delineation of effective practices does not provide requirements related to determining which type of cryptographic-based security system is appropriate for any particular

environment; those are critical and complex issues that are beyond the scope of this product. See Federal Information Processing Standard (FIPS) 140-2 and NIST 800-57 for information on more detailed cryptographic system requirements.

7.1. Cryptographic System Documentation

The strength of cryptographic systems varies widely. Having documentation of how the cryptographic features work and how they should be implemented and managed within a particular environment is critical to the long-term effectiveness of a system. It is important to establish a baseline set of materials detailing which cryptographic primitives (e.g., algorithms) the Supplier intends to implement in the proposed system and how those primitives are to be implemented and managed throughout the product life cycle.

Baseline effective practices for cryptographic system documentation:

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

- 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 system, and how these methods are to be implemented.
- The preoperational and operational phases of key establishment, deployment, ongoing validation, and revocation.

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

Cryptographic systems, once implemented, require the ability to update credentials in an efficient manner. Without these supporting capabilities, the effectiveness of the overall system will decrease over time. A process of credential updates that requires physically visiting each protected device in a very large, distributed system is unlikely to maintain its effectiveness over time. This section provides requirements for the types of functions that must be provided to enable an Acquirer to effectively manage a large number of devices installed at unattended locations.

Baseline effective practices for cryptographic system establishment, usage, and updates:

7.2.1. Use "Approved" cryptographic methods as defined in the Federal Information Processing Standard (FIPS) *Security Requirements for Cryptographic Modules* (FIPS 140-2).

7.2.2. Provide an automated remote key-establishment (update) method that protects the confidentiality and integrity of the cryptographic keys.

7.2.3. Ensure that:

- The system implementation 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 National Institute of Standards and Technology (NIST) Special Publication 800-57, Part 1 – General, *Recommendation for Key Management*.
- The key update method supports remote re-keying of all devices within [a negotiated time period(s)] as part of normal system operations.
- Emergency re-keying of all devices can be remotely performed within [a negotiated time period (e.g., 30 days)].

7.2.4. Provide a method for updating cryptographic primitives or algorithms. (Note: Prior practices have addressed updating cryptographic keys. This one addresses updates to or replacement of the cryptographic method.)

8. REFERENCES

Please refer to the original publication, *Cybersecurity Procurement Language for Energy Delivery Systems,* for a list of references used in the production of that document: http://energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf.

National Institute of Standards and Technology (NIST) Computer Security Resource Center (CRSC): https://csrc.nist.gov/

9. ABBREVIATIONS AND ACRONYMS

AAR	Association of American Railroads
ACL	Access Control List
AES	Advanced Encryption Standard
BIOS	Basic Input/Output System
C2M2	Cybersecurity Capability Maturity Model
CAPEC	Common Attack Pattern Enumeration and Classification
CEDS	Cybersecurity for Railroad Systems
CERT	Computer Emergency Response Team
CIP	Critical Infrastructure Protection
DCS	Distributed Control System
DHS	U.S. Department of Homeland Security
DMZ	Demilitarized Zone
DOE	U.S. Department of Railroad
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standard
GPS	Global Positioning System
GR	Generic Requirements
HIDS	host-based intrusion detection system
IA	Information Assurance
ICT	information and communication technology
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IDS	intrusion detection system
IETF	Internet Engineering Task Force
INFOSEC	National Information Systems Security
INL	Idaho National Laboratory
IP	Internet Protocol
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	information technology
LDAP	Lightweight Directory Access Protocol
NIDS	network intrusion detection system
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report

NTP	Network Time Protocol
OT	operations technology
OWASP	Open Web Application Security Project
RFI	request for information
RFP	request for proposal
RISC	Rail Information Security Committee
SAFECode	Software Assurance Forum for Excellence in Code
SANS	System Administration, Networking, and Security Institute
SCADA	Supervisory Control and Data Acquisition
SDLC	system development life cycle
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SP	Special Publication
SQL	Structured Query Language
SSH	Secure Shell Terminal Emulation
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
VPN	virtual private network
XSS	Cross-Site Scripting