# Appendix A: Vendor Security Response Form

See Appendix D for guidance on how to respond.

|  |  |  |  |
| --- | --- | --- | --- |
| Security Requirements – Architecture | | | |
| **#** | **Requirement** | **Please explain how the proposed solution meets the requirement or why it is not applicable** | **Specify if the product, feature, or service that meets this requirement is included in the base cost of the proposed solution**  **(Yes or No)** |
| 1.a | In the response, provide a system high level architecture diagram that includes all components and connections of the proposed solution. |  |  |
| 1.b | In the response, provide a list of the ports/protocols/services required for the proposed solution. |  |  |
| 1.c | In the response, provide a data flow diagram of the proposed solutions. |  |  |
| 1.d | Specify the Hardware, Operating System, and Software the proposed solution requires. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Requirements – Software and Services | | | |
| **#** | **Requirement** | **Please explain how the proposed solution meets the requirement or why it is not applicable** | **Specify if the product, feature, or service that meets this requirement is included in the base cost of the proposed solution**  **(Yes or No)** |
| 1.1 | The Supplier shall 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 procured product * 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 |  |  |
| 1.2 | The Supplier shall 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. |  |  |
| 1.3 | The Supplier shall 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 ports, CD/DVD drives, video ports, and serial ports). The Supplier shall provide documentation of disabled ports, connectors, and interfaces. |  |  |
| 1.4 | The Supplier shall configure the procured product to allow Tacoma Public Utilities the ability to re-enable ports and/or services if they are disabled by software. |  |  |
| 1.5 | The Supplier shall 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. |  |  |
| 1.6 | The Supplier shall provide summary documentation of the procured product’s security features and security-focused instructions on product maintenance, support, and reconfiguration of default settings. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Requirements – Access Control | | | |
| **#** | **Requirement** | **Please explain how the proposed solution meets the requirement or why it is not applicable** | **Specify if the product, feature, or service that meets this requirement is included in the base cost of the proposed solution**  **(Yes or No)** |
| 2.1 | The Supplier shall configure each component of the procured product to operate using the principle of least privilege. This includes operating system permissions, file access, user accounts, application-to-application communications, etc. |  |  |
| 2.2 | The Supplier shall provide user accounts with configurable access and permissions associated with one or more organizationally defined user role(s), where roles are used. |  |  |
| 2.3 | The Supplier shall provide a system administration mechanism for changing user(s’) role (e.g., group) associations. |  |  |
| 2.4 | The Supplier shall 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. |  |  |
| 2.5 | The Supplier shall provide a method for protecting against unauthorized privilege escalation. |  |  |
| 2.6 | The Supplier shall document options for defining access and security permissions, user accounts, and applications with associated roles. The Supplier shall configure these options, as specified by Tacoma Public Utilities. |  |  |
| 2.7 | The Supplier shall recommend methods for Tacoma Public Utilities 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. |  |  |
| 2.8 | The Supplier shall verify and provide documentation for the procured product, attesting that unauthorized logging devices (e.g., key loggers, cameras, and microphones) are not installed or are disabled, as specified by Tacoma Public Utilities. |  |  |
| 2.9 | The Supplier shall deliver a product that enables the ability for Tacoma Public Utilities 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. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Requirements – Account Management | | | |
| **#** | **Requirement** | **Please explain how the proposed solution meets the requirement or why it is not applicable** | **Specify if the product, feature, or service that meets this requirement is included in the base cost of the proposed solution**  **(Yes or No)** |
| 3.1 | The Supplier shall document all accounts (including, but not limited to, generic and/or default) that need to be active for proper operation of the procured product. |  |  |
| 3.2 | The Supplier shall change default account and password settings to Tacoma Public Utilities-specific settings (e.g., password length, complexity, history, expiration, and configurations) or support Tacoma Public Utilities in these changes. The Supplier shall not publish changed account information. The Supplier shall provide new account information to Tacoma Public Utilities via a protected mechanism. |  |  |
| 3.3 | Prior to delivery of the procured product to Tacoma Public Utilities, the Supplier shall remove or disable any accounts that are not needed for normal or maintenance operations of the procured product. |  |  |
| 3.4 | As specified by Tacoma Public Utilities, accounts for emergency operations shall be placed in a highly secure configuration and documentation on their configuration shall be provided to Tacoma Public Utilities. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Requirements – Session Management | | | |
| **#** | **Requirement** | **Please explain how the proposed solution meets the requirement or why it is not applicable** | **Specify if the product, feature, or service that meets this requirement is included in the base cost of the proposed solution**  **(Yes or No)** |
| 4.1 | The Supplier shall not permit user credentials to be transmitted or shared in clear text. The Supplier shall not store user credentials in clear text unless the Supplier and Tacoma Public Utilities agree that this is an acceptable practice for the procured product given the protection offered by other security controls. The Supplier shall only allow access protocols that encrypt or securely transmit login credentials (e.g., tunneling through Secure Shell Terminal Emulation [SSH], Transport Layer Security [TLS]). |  |  |
| 4.2 | The Supplier shall provide an appropriate level of protection (e.g., encryption and digital signing) for the session, as specified by Tacoma Public Utilities, commensurate with the technology platform, communications characteristics, and response time constraints. |  |  |
| 4.3 | Unless specifically requested by Tacoma Public Utilities, the Supplier shall 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. |  |  |
| 4.4 | The Supplier shall provide account-based and group-based configurable session-based logout and timeout settings (e.g., alarms and human-machine interfaces). |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Requirements – Authentication/Password Policy and Management | | | |
| **#** | **Requirement** | **Please explain how the proposed solution meets the requirement or why it is not applicable** | **Specify if the product, feature, or service that meets this requirement is included in the base cost of the proposed solution**  **(Yes or No)** |
| 5.1 | The Supplier shall document the levels, methods, and capabilities for authentication and authorization. The Supplier shall deliver a product that adheres to standard authentication protocols. |  |  |
| 5.2 | The Supplier shall 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 |  |  |
| 5.3 | The Supplier shall protect passwords, including not storing passwords in clear text and not hardcoding passwords into software or scripts. |  |  |
| 5.4 | The Supplier shall provide a centralized and local account management capability. |  |  |
| 5.5 | If needed for ongoing support and maintenance, the Supplier’s solutions involving interactive remote access/control shall adhere to (i.e., be compatible with) Tacoma Public Utilities’ implementation of multifactor authentication (e.g., two-factor or token). |  |  |
| 5.6 | The Supplier shall ensure that account access for single sign-on is equivalent to that enforced as a result of direct login. |  |  |
| 5.7 | The Supplier shall use a secure method of authentication (e.g., strong two-factor authentication) to allow single sign-on to a suite of applications. |  |  |
| 5.8 | The Supplier shall 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. |  |  |
| 5.9 | The Supplier shall 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. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Requirements – Logging and Auditing | | | |
| **#** | **Requirement** | **Please explain how the proposed solution meets the requirement or why it is not applicable** | **Specify if the product, feature, or service that meets this requirement is included in the base cost of the proposed solution**  **(Yes or No)** |
| 6.1 | The Supplier shall provide logging capabilities or the ability to support Tacoma Public Utilities’ existing logging system. Logging capabilities provided by the Supplier shall be configurable by Tacoma Public Utilities and support Tacoma Public Utilities’ security auditing requirements. As specified by Tacoma Public Utilities, 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 |  |  |
| 6.2 | The Supplier shall provide standard time synchronization in the procured product (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. |  |  |
| 6.3 | The Supplier shall time stamp audit trails and log files, as specified by Tacoma Public Utilities. |  |  |
| 6.4 | If required by Tacoma Public Utilities, the Supplier shall provide confidentiality and integrity security protection of log files. |  |  |
| 6.5 | The Supplier shall implement an approach for collecting and storing (e.g., transfer or log forwarding) security log files. |  |  |
| 6.6 | The Supplier shall recommend log management and Security Information and Event Management (SIEM) integration methods (e.g., syslog). |  |  |
| 6.7 | The Supplier shall 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. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Requirements – Communication Restrictions | | | |
| **#** | **Requirement** | **Please explain how the proposed solution meets the requirement or why it is not applicable** | **Specify if the product, feature, or service that meets this requirement is included in the base cost of the proposed solution**  **(Yes or No)** |
| 7.1 | The Supplier shall recommend guidance on the design and configuration of network security zones within the procured product. |  |  |
| 7.2 | The Supplier shall provide information on all communications (e.g., protocols) required between network security zones, whether inbound or outbound, and identify each network component of the procured product initiating communication. |  |  |
| 7.3 | The Supplier shall provide a method to restrict communication traffic between different network security zones. The Supplier shall provide documentation on any method or equipment used to restrict communication traffic. |  |  |
| 7.4 | The Supplier shall verify and document that disconnection points are established between the network security zones and provide the methods to isolate the zones to continue limited operations. |  |  |
| 7.5 | The Supplier shall 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. |  |  |
| 7.6 | If firewalls are provided by the Supplier, the Supplier shall provide documentation on the firewalls and their firewall rule sets for normal and emergency operations. If Tacoma Public Utilities 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. |  |  |
| 7.7 | The Supplier shall provide Tacoma Public Utilities with access, including administrative as needed, to network components of the procured product, including firewalls. |  |  |
| 7.8 | The Supplier shall document all remote access entry pathways and ensure that they can be enabled or disabled by Tacoma Public Utilities as needed. |  |  |
| 7.9 | The Supplier shall 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 Tacoma Public Utilities’ network. Where this is not available, the Supplier shall offer an alternative approach, with mitigating security measures, that is acceptable to Tacoma Public Utilities. |  |  |
| 7.10 | The Supplier shall 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. |  |  |
| 7.11 | The Supplier shall use different authentication credentials from those used for in-network communications when establishing control network access using communication tunneling. |  |  |
| 7.12 | The Supplier shall 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 shall address confidentiality and/or integrity, as specified by Tacoma Public Utilities. |  |  |
| 7.13 | The Supplier shall provide a method for managing the network components of the procured product and changing configurations, including hardware and software configurations (e.g., addressing schemes). |  |  |
| 7.14 | The Supplier shall verify and provide documentation that the network configuration management interface is secured. |  |  |
| 7.15 | The Supplier shall provide Access Control Lists (ACLs) for monitoring network components (e.g., port mirroring and network tap) of the procured product. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Requirements – Malware Detection and Protection | | | |
| **#** | **Requirement** | **Please explain how the proposed solution meets the requirement or why it is not applicable** | **Specify if the product, feature, or service that meets this requirement is included in the base cost of the proposed solution**  **(Yes or No)** |
| 8.1 | The Supplier shall provide, or specify how to implement, the capability to automatically scan any removable media that is introduced to the product being acquired. |  |  |
| 8.2 | The Supplier shall implement **at least one** of the following:   * Provide a host-based malware detection capability. The Supplier shall quarantine (instead of automatically deleting) suspected infected files. The Supplier shall provide an updating scheme for malware signatures. The Supplier shall test and confirm compatibility of malware detection application patches and upgrades. * If the Supplier is not providing the host-based malware detection capability, the Supplier shall suggest malware detection products to be used and provide guidance on malware detection and configuration settings that will work with Supplier products. * If the Supplier is not providing a host-based malware detection capability, nor suggesting malware detection products, and if specified by Tacoma Public Utilities, the Supplier shall provide an application whitelisting solution that is tested, validated, and documented that shall only permit approved applications to run. |  |  |
| 8.3 | * 1. The Supplier shall 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. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Requirements – Heartbeat Signals | | | |
| **#** | **Requirement** | **Please explain how the proposed solution meets the requirement or why it is not applicable** | **Specify if the product, feature, or service that meets this requirement is included in the base cost of the proposed solution**  **(Yes or No)** |
| 9.1 | The Supplier shall 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. |  |  |
| 9.2 | The Supplier shall provide packet definitions of the heartbeat signals and examples of the heartbeat traffic if the signals are included in network monitoring. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Requirements – Reliability and Adherence to Standards | | | |
| **#** | **Requirement** | **Please explain how the proposed solution meets the requirement or why it is not applicable** | **Specify if the product, feature, or service that meets this requirement is included in the base cost of the proposed solution**  **(Yes or No)** |
| 10.1 | The Supplier shall protect the confidentiality and integrity of Tacoma Public Utilities’ sensitive information. |  |  |
| 10.2 | The Supplier shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput specified. |  |  |
| 10.3 | The Supplier shall use an implementation that complies with the current applicable interoperability and security standards, as specified by Tacoma Public Utilities (e.g., NIST 800 series, ISA/IEC 62443, IEEE 1613, IEEE 1588, and NERC CIP). |  |  |
| 10.4 | Upon Tacoma Public Utilities’ request, the Supplier shall return or document the secure disposal of Tacoma Public Utilities’ data and Tacoma Public Utilities-owned hardware that is no longer needed by the Supplier (e.g., NIST Special Publication [SP] 800-80). |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Requirements – Secure Development Practices | | | |
| **#** | **Requirement** | **Please explain how the proposed solution meets the requirement or why it is not applicable** | **Specify if the product, feature, or service that meets this requirement is included in the base cost of the proposed solution**  **(Yes or No)** |
| 11.1 | The Supplier shall provide summary documentation of its 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 energy delivery system hardware, software, and firmware. If applicable, the Supplier shall document how the most critical application security weaknesses (including *OWASP Top 10* or *SANS Top 25 Most Dangerous Software Errors*) are addressed in the Supplier’s SDLC. |  |  |
| 11.2 | As specified by Tacoma Public Utilities, the Supplier shall identify the country (or countries) of origin of the procured product and its components (including hardware, software, and firmware). The Supplier shall identify the countries where the development, manufacturing, maintenance, and service for the product are provided. The Supplier shall notify Tacoma Public Utilities 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. |  |  |
| 11.3 | The Supplier shall 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. The Supplier shall 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. The Supplier shall provide summary documentation of the results of the testing that includes unresolved vulnerabilities and recommended mitigation measures. |  |  |
| 11.4 | The Supplier shall provide summary documentation of its coding reviews, including defect lists and plans to correct identified vulnerabilities. |  |  |
| 11.5 | The Supplier shall 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 Tacoma Public Utilities. The Supplier shall communicate with Tacoma Public Utilities within [a negotiated time period] (see Section 3.3.3). This is not intended for nontechnical contract-related issues. |  |  |
| 11.6 | The Supplier shall 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. |  |  |
| 11.7 | The Supplier shall 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). |  |  |
| 11.8 | Tacoma Public Utilities 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 Tacoma Public Utilities. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Requirements – Documentation and Tracking of Vulnerabilities | | | |
| **#** | **Requirement** | **Please explain how the proposed solution meets the requirement or why it is not applicable** | **Specify if the product, feature, or service that meets this requirement is included in the base cost of the proposed solution**  **(Yes or No)** |
| 12.1 | Upon request of Tacoma Public Utilities, and prior to the delivery of the procured product, the Supplier shall provide summary documentation of publicly disclosed vulnerabilities in the procured product and the status of the Supplier’s disposition of those publicly disclosed vulnerabilities. |  |  |
| 12.2 | The Supplier shall provide, within [a negotiated time period] after product delivery, summary documentation of uncorrected security vulnerabilities in the procured product. This includes summary documentation 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, mitigations, and/or procedural workarounds. |  |  |
| 12.3 | After contract award, the Supplier shall 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. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Requirements – Problem Reporting | | | |
| **#** | **Requirement** | **Please explain how the proposed solution meets the requirement or why it is not applicable** | **Specify if the product, feature, or service that meets this requirement is included in the base cost of the proposed solution**  **(Yes or No)** |
| 13.1 | The Supplier shall provide a secure process for users to submit problem reports and remediation requests. This process shall include tracking history and corrective action status reporting. |  |  |
| 13.2 | Upon Tacoma Public Utilities submitting a problem report to the Supplier, 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 Tacoma Public Utilities within [a negotiated time period]. |  |  |
| 13.3 | The Supplier shall provide Tacoma Public Utilities 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. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Requirements – Patch Management and Updates | | | |
| **#** | **Requirement** | **Please explain how the proposed solution meets the requirement or why it is not applicable** | **Specify if the product, feature, or service that meets this requirement is included in the base cost of the proposed solution**  **(Yes or No)** |
| 14.1 | The Supplier shall provide documentation of its 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 Tacoma Public Utilities. This documentation shall also include the Supplier’s approach and capability to remediate newly reported zero-day vulnerabilities. |  |  |
| 14.2 | The Supplier shall 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 Tacoma Public Utilities, or within [a pre-negotiated period] after delivery. |  |  |
| 14.3 | 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]. |  |  |
| 14.4 | When third-party hardware, software, and firmware is provided by the Supplier to Tacoma Public Utilities, 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]. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Requirements – Supplier Personnel Management | | | |
| **#** | **Requirement** | **Please explain how the proposed solution meets the requirement or why it is not applicable** | **Specify if the product, feature, or service that meets this requirement is included in the base cost of the proposed solution**  **(Yes or No)** |
| 15.1 | The Supplier shall provide summary documentation to attest to its workforce receiving position-appropriate cybersecurity training and awareness. This includes specialized training for those involved in the design, development, manufacture, testing, shipping, installation, operation, and maintenance of products procured by Tacoma Public Utilities, as part of the Supplier’s cybersecurity program. |  |  |
| 15.2 | The Supplier shall perform security background checks on its employees (including contract personnel) working directly on or involved in the development of a Tacoma Public Utilities’ system or procured product. The background check methodology shall be mutually agreed upon by Tacoma Public Utilities and Supplier. |  |  |
| 15.3 | The Supplier shall ensure that policies and procedures are followed to prohibit the unauthorized disclosure of knowledge, information, architectures, or configuration relevant to Tacoma Public Utilities’ system. |  |  |
| 15.4 | The Supplier shall share information with Tacoma Public Utilities to support the timely update of authentication credentials and access control to reflect staffing changes. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Requirements – Secure Hardware and Software Delivery | | | |
| **#** | **Requirement** | **Please explain how the proposed solution meets the requirement or why it is not applicable** | **Specify if the product, feature, or service that meets this requirement is included in the base cost of the proposed solution**  **(Yes or No)** |
| 16.1 | The Supplier shall establish, document, and implement risk management practices for supply chain delivery of hardware, software, and firmware. The Supplier shall 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 |  |  |
| 16.2 | The Supplier shall 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 Tacoma Public Utilities deems that it is warranted, the Supplier shall apply encryption to protect procured products throughout the delivery process. |  |  |
| 16.3 | The Supplier shall use trusted channels to ship technology system hardware, such as U.S. registered mail. |  |  |
| 16.4 | The Supplier shall demonstrate a capability for detecting unauthorized access throughout the delivery process. |  |  |
| 16.5 | The Supplier shall demonstrate chain-of-custody documentation for technology system hardware and require tamper-evident packaging for the delivery of this hardware. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Requirements – General Wireless Technology Provisions | | | |
| **#** | **Requirement** | **Please explain how the proposed solution meets the requirement or why it is not applicable** | **Specify if the product, feature, or service that meets this requirement is included in the base cost of the proposed solution**  **(Yes or No)** |
| 17.1 | The Supplier shall 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. |  |  |
| 17.2 | The Supplier shall document use, capabilities, and limits for the wireless devices. |  |  |
| 17.3 | 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). |  |  |
| 17.4 | The Supplier shall document the range of the wireless devices and verify that the range of communications is minimized to both meet the needs of Tacoma Public Utilities’ proposed deployment and reduce the possibility of signal interception. |  |  |
| 17.5 | The Supplier shall 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). |  |  |
| 17.6 | The Supplier shall 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. |  |  |
| 17.7 | The Supplier shall document the configuration control options that enable varying of the security level of the devices. |  |  |
| 17.8 | The Supplier shall allow and recommend alarm settings in accordance with the needs of the system. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Requirements – Cryptographic System Documentation | | | |
| **#** | **Requirement** | **Please explain how the proposed solution meets the requirement or why it is not applicable** | **Specify if the product, feature, or service that meets this requirement is included in the base cost of the proposed solution**  **(Yes or No)** |
| 18.1 | The Supplier shall 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 Tacoma Public Utilities. 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. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Requirements – Cryptographic Key and Method Establishment, Usage and Update | | | |
| **#** | **Requirement** | **Please explain how the proposed solution meets the requirement or why it is not applicable** | **Specify if the product, feature, or service that meets this requirement is included in the base cost of the proposed solution**  **(Yes or No)** |
| 19.1 | The Supplier shall only use “Approved” cryptographic methods as defined in the Federal Information Processing Standard (FIPS) *Security Requirements for Cryptographic Modules* (FIPS 140-2). |  |  |
| 19.2 | The Supplier shall provide an automated remote key-establishment (update) method that protects the confidentiality and integrity of the cryptographic keys. |  |  |
| 19.3 | The Supplier shall 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 NIST 800-57 Part 1. * 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)]. |  |  |
| 19.4 | The Supplier shall provide a method for updating cryptographic primitives or algorithms. (Note: Prior requirements have addressed updating cryptographic keys. This requirement addresses updates to or replacement of the cryptographic method.) |  |  |