The Control Systems FAT and SAT Checklist is based on the DHS Cybersecurity Procurement Language for Control Systems Rev 4, augmented with new DoD guidance from the Unified Facility Criteria, UFC 4-010-06 Cybersecurity Of Facility-Related Control Systems 2016, and the DoD Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DoD) Industrial Control Systems (ICS) 2016.

Factory Acceptance Test Measures: The Factory Acceptance Test (FAT) is necessary to verify that security features function properly and provide the expected levels of functionality. Each topic includes FAT tasks specific to that topic. In general, prior to initiation of each FAT, the Vendor shall install all operating systems and application patches, service packs, or other updates certified for use with the provided system by the time of test, and documentation of the configuration baseline. FAT is a process, not an event, and could in fact extend over several weeks or months.

Site Acceptance Test Measures: The asset Purchaser's Site Acceptance Test (SAT) typically repeats a subset of a FAT after system installation with additional integrated functions. Typically, the SAT is performed before the cutover or commissioning to validate that the site installation is equivalent to the system tested at the factory. Like the FAT, the SAT may extend several weeks or months and may occur at multiple locations.

PERFORMANCE REQUIREMENT	RATIONAL	FAT Submittal	FAT Measures	SAT Submittal	SAT Measures
1. TEST AND DEVELOPMENT ENVIRONMENT	A Test and Development Environment (TDE) is as close a mirror to the production control system environment as possible where software/firmware updates, patches, new equipement, new configurations, and operational procedures can be tested and verified prior to implementing in the Production Environment.				
1.1 Create the Test and Development Environment	For new or major modernization projects, the Systems Integrator will establish a Test and Development Environment (TDE) that replicates the Production Environment to the highest degree possible starting with the Level 4 Workstations, Servers, software and with at least one of each of the Level 3-0 major components, devices, and actuators. For minor projects or on-going operations and maintenance replacement, use the existing Platform Enclave Operations Center TDE.	NA	At approximately the 50-75% construction complete, the TDE will be used to perform Factory Acceptance Testing (FAT) of the project to ensure the project has end-to-end functionality, has been properly configured using the Security Content Automation Protocol (SCAP) tool and the Security Technical Implementation Guides (STIGS), all patches (OS and CS) are installed and properly configured, and begin creating the artifacts for the draft System Security Plan.	NA	At approximately 95-100% construction complete, the TDE will be used to conduct Site Acceptance Testing of the complete CS, and if required, Penetration testing. The SAT artifacts will be included in the final System Security Plan, FMC and Jump-Kit (if required). The Project Team/System Integrator will transfer the TDE to the Government PM for inclusion into the Platform Enclave Operations Center.

1.2 Penetration Testing	NIST SP 800-82R2 CA-8 Penetration Testing - Penetration testing is used with care on CS networks to ensure that CS functions are not adversely impacted by the testing process. In general, CS are highly sensitive to timing constraints and have limited resources. Example compensating controls include employing a replicated, virtualized, or simulated system to conduct penetration testing. Production CS may need to be taken off-line before testing can be conducted. If CS are taken off-line for testing, tests are scheduled to occur during planned CS outages whenever possible. If penetration testing is performed on non-CS networks, extra care is taken to ensure that tests do not propagate into the CS network.	Yes	The Vendor shall verify that the Purchaser requires the results of Penetration Testing (typically only for High Impact systems). Complete the PenTesting Rules of Engagement form and completed FAT Pen Test Checklist.	Yes	The Vendor shall verify that the Purchaser requires the results of Penetration Testing (typically only for High Impact systems). Complete the PenTesting Rules of Engagement form and completed SAT Pen Test Checklist.
2. SYSTEM HARDENING	System hardening refers to making changes to the default configuration of a network device and its operating system (OS), software applications, and required third-party software to reduce system security vulnerabilities.				
2.1 Removal of Unnecessary Services and Programs	Unnecessary services and programs are often installed on network devices.	Yes	The Vendor shall verify that the Purchaser requires the results of cyber security scans (as a minimum a vulnerability and active port scan, with the most current signature files) run on the control system as a primary activity of the FAT. This assessment is then compared with an inventory of the required services, patching status, and documentation, to validate this requirement.	Yes	The Vendor shall compare the results of cyber security scans run on the system, as a primary activity of the SAT, with an inventory of the required services, patching status, and required documentation. At the conclusion of the SAT and before cutover or commissioning, the above cyber security scans (with the most current signature files) must be run again.

2.2 Host Intrusion Detection System	A host intrusion detection system (HIDS) can be installed to perform a variety of integrity checks to detect attempted unauthorized access.	Yes	The Vendor shall verify and provide documentation that for Vendor-supplied HIDS; the Vendor shall run the HIDS during the entire FAT process and periodically interject applicable malware. The Vendor shall examine log files and validate the expected results. FAT procedures shall include validation and documentation of this requirement.	Yes	The Vendor shall verify and provide documentation that for Vendor-supplied HIDS. The Vendor shall run the HIDS during the entire SAT process and periodically interject applicable malware. The Vendor shall examine log files and validate the expected results. SAT procedures shall include validation and documentation of this requirement. The Vendor shall generate a system image at the conclusion of the SAT to be used later as a control baseline.
2.3 Changes to File System and Operating System Permissions	Hardening file system configurations and restricting operating system permissions reduce the vulnerabilities associated with default configurations.	Yes	The Vendor shall provide, as a part of the FAT procedures, validation and documentation of the permissions assigned.	Yes	The Vendor shall provide, as a part of the SAT procedures, validation and documentation of the permissions assigned.
2.4 Hardware Configuration	Unnecessary hardware can be physically disabled, removed, or its configuration altered through software.	Yes	The Vendor shall provide, as a part of the FAT procedures, validation and documentation of the disabled or locked physical access and the removed drivers.	Yes	The Vendor shall provide, as a part of the SAT procedures, validation and documentation of the disabled or locked physical access and the removed drivers.
2.5 Heartbeat Signals	Heartbeat signals indicate the communication health of the system.	Yes	The Vendor shall provide, as a part of the FAT procedures, documentation of the requirements. The Vendor shall create a baseline of the heartbeat communications traffic, to include frequency, packet sizes, and expected packet configurations.	Yes	The Vendor shall provide, as a part of the SAT procedures, documentation of the requirements. The Vendor shall create a baseline of the heartbeat communications traffic and validate the results against FAT documentation
2.6 Installing Operating Systems, Applications, and Third-Party Software Updates	Patches and software updates, including those for anti-virus scanners, are required to reduce attack surface.	Yes	The Vendor shall install and update all tested and validated security patches prior to the start of the FAT. The Vendor shall verify and provide documentation that all updates have been tested and installed. The Vendor shall perform contractually agreed upon security scans (with the most current signature files) to verify that the system has not been compromised during the testing phase. The Vendor shall provide documentation of the results of the scans. The Vendor shall document the system after the FAT to support future validation of patches. (In many instances, this is referred to as the system baseline.)	Yes	The Vendor shall install and update all tested and validated security patches at the start of the SAT. The Vendor shall provide documentation that all the updates have been tested and installed. The Vendor shall verify system functionality, based on pre-negotiated procedures, at the conclusion of patch updates, and provide documentation of the results. The Vendor shall perform security scans (with the most current signature files) to verify that the system has not been compromised during the testing phase of the results. The Vendor shall document the system after the SAT to support future validation of patches. (In many instances, this is referred to as delivered system configuration.)

3. PERIMETER PROTECTION	Perimeter protection refers to providing a clear demarcation between the protected internal network and unprotected and untrusted external networks.				
3.1 Firewalls	Firewalls are used to stop unauthorized connections, or to allow limited communications between two networks or from a network to a networked device. Firewalls fall into four broad categories: packet filters, circuit level gateways, application level gateways, and stateful multilayer inspection firewalls. Firewalls can be implemented in software, hardware, or a combination of both.	Yes	The Vendor shall install the firewall(s) or the configuration(s) and run the firewall(s) continuously during the entire FAT process for Vendor-supplied firewall(s), or Vendor-provided firewall configuration(s). The Vendor shall verify that FAT procedures include exercising this functionality, examining the log files, and validating the results. The Vendor shall verify that FAT procedures include validation and documentation of the requirements.	Yes	The Purchaser shall run the firewall(s) during the entire SAT process. The Vendor shall verify that SAT procedures include exercising this functionality, examining the log files, and validating the results. The Vendor shall verify that SAT procedures include validation and documentation of the requirements. Any Vendor-configured or manufacturer default usernames, passwords, or other security codes must be changed at this time.
3.2 Network Intrusion Detection System	A NIDS is used to identify unauthorized or abnormal network traffic.	Yes	The Vendor shall install the NIDS or the configuration(s) and run the NIDS continuously during the entire FAT process for Vendor-supplied NIDSs, or Vendor-provided NIDS configuration(s). The Vendor shall verify that FAT procedures include exercising this functionality, examining the log files, and validating the results. The Vendor shall verify that FAT procedures include validation and documentation of the requirements.	Yes	The Vendor shall run the NIDS(s) during the entire SAT process to include exercising this functionality, examining the log files, and validating the results. The Vendor shall document the results of tuning signatures and adjusting thresholds to reduce false positives and minimize false negatives. The Vendor shall verify that SAT procedures include validation and documentation of the requirements. Any Vendor-configured or manufacturer default usernames, passwords, or other security codes must be changed at this time.
3.3 Canaries	Honey pots (which analyze unauthorized connections) and/or Canary(ies) (which flag that a connection attempt has taken place) have been implemented in certain network configurations to provide passive network monitoring.	Yes	The Vendor shall install the canary(ies) or the configuration(s) and run the canary(ies) continuously during the entire FAT process for Vendor-supplied canary(ies) or Vendor-provided canary configuration(s). The Vendor shall verify that FAT procedures include exercising this functionality, examining the log files, and validating the results. The Vendor shall verify that FAT procedures include written validation and documentation of the requirements.	Yes	The Vendor shall run the canary(ies) during the entire SAT process. The Vendor shall verify that SAT procedures include exercising this functionality, examining the log files, and validating the results. The Vendor shall verify that SAT procedures include written validation and documentation of the requirements. Any Vendor-configured or manufacturer default usernames, passwords, or other security codes must be changed at this time
4. ACCOUNT MANAGEMENT	Account management is essential to properly maintain and secure a control systems network. Account management regulates who has access, limits permission to only those required, and mitigates vulnerabilities in default accounts. It also covers password management.				

4.1 Disabling, Removing, or Modifying Well-Known or Guest Accounts	Disabling, removing, or modifying well-known or guest accounts and changing default passwords are necessary to reduce system vulnerabilities.	Yes	The Vendor shall verify that FAT procedures include exercising this functionality, examining the log files, and validating the results. The Vendor shall verify that FAT procedures include written validation and documentation of the requirements.	Yes	The Vendor shall verify that SAT procedures include exercising this functionality, examining the log files, and validating the results. The Vendor shall verify that SAT procedures include written validation and documentation of the requirements
4.2 Session Management	Weak session practices and insecure protocols exist on many systems for convenience, backwards compatibility, and on legacy systems.	Yes	The Vendor shall verify that FAT procedures include validation and documentation of the requirements.	Yes	The Vendor shall verify that SAT procedures include validation and documentation of the requirements.
4.3 Password/Authentication Policy and Management	Instant availability requirements in control systems often result in a weak password policy.	Yes	The Vendor shall verify that FAT procedures include validation and documentation of the password and authentication policy and management.	Yes	The Vendor shall verify that SAT procedures include validation and documentation of the password and authentication policy and management.
4.4 Account Auditing and Logging	Account auditing and logging allow the Purchaser/Operator to verify that authorized operations have been maintained. Logging is also necessary for forensic analysis and anomaly detection.	Yes	The Vendor shall verify that FAT procedures include validation and documentation of the requirements. The Vendor shall record system performance measurements that include the system with and without logging activities.	Yes	The Vendor shall verify that SAT procedures include validation and documentation of the requirements. The Vendor shall record system performance measurements to verify that logging activities do not adversely impact system performance.
4.5 Role-Based Access Control for Control System Applications	Role-based access control (RBAC) refers to the system's ability to make access decisions based on the role(s) of individual users/processes in the control system environment. Using RBAC results in significant improvements in security. The use of roles to control access can be an effective means for developing and enforcing systemwide security policies and for streamlining security management processes. RBAC limits the exposure to risk associated with unauthorized actions by assigning the least privileges corresponding to the assigned duty or function. The use of RBAC for administrative functions is not common on legacy systems.	Yes	The Vendor shall compare the control system assessment during this period with required documentation to validate the requirements. The Vendor shall baseline user roles and permissions and negotiate agreements on modifications with the system Purchaser/Operators.	Yes	The Vendor shall verify that all additions to the control system, after the completion of the FAT, have the same rigor of documentation that was necessary pre-FAT and appropriate comparisons are required post-SAT to validate the requirement.

4.6 Single Sign-On	Single sign-on (SSO) refers to a means of user authentication such that a single login allows a user to have authorized role-based access across a network or between programs and systems, without requiring re-authentication to each application.	Yes	The Vendor shall verify that FAT procedures include validation and documentation that the SSO permissions and session management are handled properly.	Yes	The Vendor shall verify that SAT procedures include validation and documentation that the SSO permissions and session management are handled properly.
4.7 Separation Agreement	The Purchaser needs to have agreements with Vendors to protect their control systems security posture.	Yes	The Vendor shall verify that FAT procedures include validation and documentation of the ability to change key employee/support personnel access and permissions.	Yes	The Vendor shall verify that SAT procedures include validation and documentation of the ability to change key employee/support personnel access and permissions.
5. CODING PRACTICES	Secure coding practices refer to techniques for building and validating high levels of security into software, beginning at the requirements phase, implemented during the coding phase, and finally validated during the FAT and SAT.				
5.1 Coding for Security	Standard programming texts generally address data processing, but not security ramifications; this may mislead programmers into writing insecure code.	Yes	The Vendor shall verify that FAT procedures include validation and documentation of the software development process and/or code review.	Yes	The Vendor shall verify that SAT procedures include validation and documentation of the software development process and/or code review.
6. FLAW REMEDIATION	Flaw remediation refers to the actions to be performed and documentation to be produced when flaws are discovered in control system software, hardware, and system architectures created by or under the control of the Vendor.				
6.1 Notification and Documentation from Vendor	Flaw remediation is a process by which flaws are documented and tracked for completion of corrective actions.	Yes	The Vendor shall verify that for flaws known by the Vendor, the Vendor's corrective actions follow their process and the process is effective. The Vendor shall verify that FAT documentation of the flaws validation and remediation are provided. The Vendor shall verify that any changes to the core system code, logic, or configuration are analyzed to verify new vulnerabilities are not introduced into the system as a result of the change.	Yes	The Vendor shall verify that for flaws known by the Vendor, the Vendor's corrective actions follow their process and the process is effective. The Vendor shall verify that SAT documentation of the flaws validation and repair are provided. The Vendor shall verify that any changes to the core system code, logic, or configuration are analyzed to verify new vulnerabilities are not introduced into the system as a result of the change.

6.2 Problem Reporting	Vulnerabilities exist in core logic and configuration of control systems. When flaws in software and/or hardware configuration are discovered by users, the Vendor shall have a process in place by which the user can report such flaws. A flaw remediation process shall be used to track progress of patches, fixes, and workarounds until completion.	Yes	None.	Yes	None.
7. MALWARE DETECTION AND PROTECTION	Malware is any unauthorized software. Because many control networks are connected to other networks or updated by media, malware can enter into the network and affect process control and/or communications. Malware consists of many different types of software and may include, but is not limited to, bots, Trojans, worms, viruses, backdoors, and zombies. Malware detection can occur on a host or a network-based device.				
7.1 Malware Detection and Protection	Updates to malware detection software may adversely impact control system behavior.	Yes	The Vendor shall record system performance measurements that include the system with and without malware detection. The Vendor shall verify all media and equipment are scanned under the most current malware detection versions available prior to onsite transport. The Vendor shall exercise the malware detection system. The Vendor shall document any known or identified backdoor codes.	Yes	The Vendor shall record system performance measurements to verify that malware detection does not adversely impact system performance. The Vendor shall document any known or identified backdoor codes.
8. HOST NAME RESOLUTION	The Domain Name System (DNS) performs a key function in IP networks by providing name resolution services, translating computer names to IP addresses, and translating IP addresses to computer names. DHCP is often used in conjunction with the DNS server to assign IP addresses to client computers. DHCP allows the IP allocation to be completed dynamically with the address expiring after a predetermined length of time.				

8.1 Network Addressing and Name Resolution	Each computer in a network has a unique IP address. Remembering each address for each computer in a network is difficult, so addresses are often mapped to host names, which are easier to remember. DNS servers translate the host name used by people to the IP address used by computers. IP addresses can be assigned statically or can be allocated dynamically from a pool of addresses using DHCP. The most widely used DNS software is Berkeley Internet Name Domain (BIND) produced by Internet Software Consortium (ISC), although other packages exist, including Microsoft DNS.	Yes	The Vendor shall install and run Vendor-supplied DNS servers continuously during the entire FAT process. The Vendor shall verify all domain servers, and hosts within the domain involved in testing are resolvable by all client and server systems connected to the network. The Vendor shall document both forward (hostname to IP address) resolution and reverse (IP address to hostname) resolution.	Yes	The Vendor shall run the DNS server during the entire SAT process. The Vendor shall verify all domain servers and hosts within the domain involved in testing are resolvable by all client and server systems connected to the network. The Vendor shall document both forward (hostname to IP address) resolution and reverse (IP address to hostname) resolution.
9. END DEVICES	End devices refer to components in the control system that gather information or control a process. These could include sensors, controllers, valves, processors, etc. Network and security architectures will change during the long lifespan of end devices, which necessitates detailed end device specifications (e.g., latency, calibrations, protocols, interoperability, and default security settings).				

9.1 Intelligent Electronic Devices	An intelligent electronic device (IED) is sometimes referred to as an intelligent end device. It incorporates microprocessors within the device, receives information from process sensors or from the power equipment, and issues control commands to process equipment such as breakers, valves, pumps, transformers, etc.	Yes	The Vendor shall verify and provide documentation of physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use. The Vendor shall verify and provide documentation that all validated security updates and patches are installed and tested at the start of the FAT. The Vendor shall verify and provide documentation that all unused software and services are removed or disabled. Post-FAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to, cyber security features, software, protocols, ports, and services and provide documentation describing each item. The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput for field communications. The Vendor shall verify that FAT procedures include validation and documentation of the requirements.	Yes	The Vendor shall verify and provide documentation of any changes to physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use. Post-SAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to, cyber security features, software, protocols, ports, and services and provide documentation describing any changes. The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed at the start of the SAT.

9.2 Remote Terminal Units	A remote terminal unit (RTU) is a microprocessor-controlled device that is used to provide system control of industrial processes.	Yes	The Vendor shall verify and provide documentation of physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use. The Vendor shall verify and provide documentation that all validated security updates and patches are installed and tested at the start of the FAT. The Vendor shall verify and provide documentation that all unused software and services are removed or disabled. Post-FAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to, cyber security features, software, protocols, ports, and services and provide documentation describing each item. The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput. The Vendor shall verify that FAT procedures include validation and documentation of the requirements.	Yes	The Vendor shall verify and provide documentation of changes to physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use. Post-SAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to, cyber security features, software, protocols, ports, and services and provide documentation describing any changes. The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed at the start of the SAT. The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput when connected during the SAT. The Vendor shall verify that SAT procedures include validation and documentation of the requirements.

9.3 Programmable Logic Controllers	A PLC is a digital computer used to provide system control of industrial processes. PLCs are designed for multiple inputs and outputs along with a processing unit used to monitor inputs, make decisions, and control outputs.	Yes	The Vendor shall verify and provide documentation of physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use. The Vendor shall verify and provide documentation that all validated security updates and patches are installed and tested at the start of the FAT. The Vendor shall verify and provide documentation that all unused software and services are removed or disabled. Post-FAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to, cyber security features, software, protocols, ports, and services and provide documentation describing each item. The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput. The Vendor shall verify that FAT procedures include validation and documentation of the requirements.	Yes	The Vendor shall verify and provide documentation of and changes to physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use. Post-SAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to, cyber security features, software, protocols, ports, and services and provide documentation describing any changes. The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed at the start of the SAT. The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput when connected during the SAT. The Vendor shall verify that SAT procedures include validation and documentation of the requirements.

9.4 Sensors, Actuators, and Meters	Sensors, actuators, and meters are traditionally dumb devices that produce outputs or accept inputs from a control system. The trend is toward sensors, actuators, and meters that incorporate microprocessors, also known as “smart devices.” “Smart” sensors are also referred to as “smart transducers.”	Yes	The Vendor shall verify and provide documentation of physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use. Post-FAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to, cyber security features, software, protocols, ports and services and provide documentation describing each item. The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput. The Vendor shall verify that FAT procedures include validation and documentation of the requirements. For smart devices: • The Vendor shall verify and provide documentation that all validated security updates and patches are installed and tested at the start of the FAT. • The Vendor shall verify and provide documentation that all unused software and services are removed or disabled.	Yes	The Vendor shall verify and provide documentation of and changes to physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use. Post-SAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to cyber security features, software, protocols, ports and services and provide documentation describing any changes. The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput when connected during the SAT. The Vendor shall verify that SAT procedures include validation and documentation of the requirements. For smart devices: • The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed at the start of the SAT. •
10. REMOTE ACCESS	Remote access refers to the ability to connect to a computer or network from a different location via modem, Ethernet, serial, TCP/IP, VPN, or wireless.				

10.1 Dial-Up Modems	Dial-up modems allow remote access to control system equipment.	Yes	The Vendor shall verify and provide documentation of physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use. The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput. Post-FAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing each item. The Vendor shall verify and provide documentation that all validated security updates and patches are installed and tested at the start of the FAT. The Vendor shall verify and provide documentation that all unused software and services are removed or disabled. The Vendor shall provide a summary table indicating each communication path required by the system. The Vendor shall perform network-based validation and documentation steps on each device including full TCP and UDP port scans. The Vendor shall complete the cyber security scans during a	Yes	The Vendor shall verify and provide documentation of and changes to physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use. Post-SAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to, cyber security features, software, protocols, ports, and services and provide documentation describing any changes. The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed at the start of the SAT. The Vendor shall perform war dialing or discovery activities and provide documentation of the results. The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput when connected during the SAT. The Vendor shall verify that SAT

10.2 Dedicated Line Modems	Modems allow remote access to control system equipment.	Yes	The Vendor shall verify and provide documentation of physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use. The Vendor shall verify and provide documentation that all validated security updates and patches are installed and tested at the start of the FAT. The Vendor shall verify and provide documentation that all unused software and services are removed or disabled. Post-FAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to, cyber security features, software, protocols, ports, and services and provide documentation describing each item. The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput. The Vendor shall provide a summary table indicating each communication path required by the system. The Vendor shall perform network-based validation and documentation steps on each device, including full TCP and UDP port scans. The Vendor shall complete the cyber security scans during a	Yes	The Vendor shall verify and provide documentation of and changes to physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use. Post-SAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to cyber security features, software, protocols, ports and services and provide documentation describing any changes. The Vendor shall perform discovery activities and provide documentation of the results. The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed at the start of the SAT. The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput when connected during the SAT. The Vendor shall verify that SAT

10.3 TCP/IP	The TCP/IP stack is the foundation of communication on the Internet and most commercial networks. It is named after its two most important protocols: the IP and the TCP. Other important IPs include UDP, Address Resolution Protocol (ARP), and Internet Control Message Protocol (ICMP). IP operates at the network layer of a network and provides connectionless unreliable communication. IP is responsible for sending and routing packets, but is connectionless and does not guarantee transmission. TCP runs on top of the IP and provides connection-oriented reliable communication.	Yes	The Vendor shall verify and provide documentation of physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the system from unauthorized modification or use. The Vendor shall verify and provide documentation that all validated security updates and patches are installed and tested at the start of the FAT. The Vendor shall verify and provide documentation that all unused software and services are removed or disabled. Post-FAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to cyber security features, software, protocols, ports and services and provide documentation describing each item. The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput. The Vendor shall provide documentation of the results of the independent third-party security validation of the IPv6 implementations. The Vendor shall verify that FAT procedures include validation and documentation of the requirements.	Yes	The Vendor shall verify and provide documentation of and changes to physical and cyber security features, including but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the system computer from unauthorized modification or use. Post-SAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to, cyber security features, software, protocols, ports, and services and provide documentation describing any changes. The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed at the start of the SAT. The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput when connected during the SAT. The Vendor shall verify that SAT procedures include validation and documentation of the requirements.

10.4 Web-based Interfaces	Many control systems have Web-based interfaces for performing some tasks.	Yes	The Vendor shall verify and provide documentation of physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the system from unauthorized modification or use. The Vendor shall verify and provide documentation that all validated security updates and patches are installed and tested at the start of the FAT. The Vendor shall verify and provide documentation that all unused software and services are removed or disabled. Post-FAT, the Vendor shall create a baseline of all communications to and from any device running an HTTP server and configuration including, but not limited to cyber security features, Web-based interfaces, software, protocols, ports, and services and provide documentation describing the functionality of each item. The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput. The Vendor shall provide documentation of the results of the independent third-party security code validation for all Web application and Web server software. The Vendor shall verify that FAT procedures include validation	Yes	The Vendor shall verify and provide documentation of and changes to physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the system from unauthorized modification or use. Post-SAT, the Vendor shall create a baseline of all communications to and from any device running an HTTP server and configuration including, but not limited to, cyber security features, Web based interfaces, software, protocols, ports, and services and provide documentation describing any changes. The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput when connected during the SAT. The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed at the start of the SAT. The Vendor shall verify and provide documentation that all unused software and

10.5 Virtual Private Networks	Virtual private networks (VPNs) allow for secure or trusted communications over an unsecured or untrusted infrastructure such as the Internet. The advantages of such systems are confidentiality, integrity, and availability. A poorly configured VPN creates easily exploitable vulnerabilities. The term VPN is a very large category that includes any mechanism that creates a logical division where there is not a physical division of a network. This situation creates a subnetwork that is not accessible by members of the network who are not part of the subnetwork. This large category encroaches on the category of network partitioning. This section will concentrate on the subcategory of VPN limited to the encrypted tunneling of traffic through untrusted networks. Examples of where this type of VPN is useful are: • Site-to-site control system	Yes	The Vendor shall verify and provide documentation of physical and cyber security features including, but not limited to, multifactor authentication (e.g., security token, known key, and/or certificate), encryption, access control, event and communication logging, monitoring, and alarming to protect the system and configuration computer from unauthorized modification or use. The Vendor shall verify and provide documentation that all validated security updates and patches are installed and tested at the start of the FAT. The Vendor shall create a baseline of the delivered system communications and configuration including, but not limited to, cyber security features, software, protocols, ports, and services and provide documentation describing each item. Post-FAT, the Vendor shall create a baseline of the delivered system communications and configuration including, but not limited to, cyber security features, Web-based interfaces, software, protocols, ports, and services and provide documentation describing the functionality of each item. The Vendor shall verify and provide documentation that all unused software and services are removed or disabled. The Vendor shall verify that FAT procedures include validation and documentation of the requirements.	Yes	The Vendor shall verify and provide documentation of and changes to physical and cyber security features, including but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use. Post-SAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to, cyber security features, software, protocols, ports, and services and provide documentation describing any changes. The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed at the start of the SAT. The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput when connected during the SAT. The Vendor shall verify that SAT procedures include validation and documentation of the requirements.

10.6 Serial Communications Security	Many protocols are used for both serial and Ethernet communications.	Yes	The Vendor shall verify and provide documentation of physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the serial communications and communication devices from unauthorized modification or use. The Vendor shall provide documentation of the independent third-party validation of all software running on field communication devices (see Section 5.1). The Vendor shall verify and provide documentation that all validated security updates and patches are installed and tested at the start of the FAT. The Vendor shall verify and provide documentation that all unused software and services are removed or disabled. Post-FAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to, cyber security features, software, protocols, ports and services and provide documentation describing each item. The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput. The Vendor shall verify that FAT procedures include validation and documentation of the requirements.	Yes	The Vendor shall verify and provide documentation of any changes to physical and cyber security features including, but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use. Post-SAT, the Vendor shall create a baseline of all serial communications and configuration including, but not limited to, cyber security features, software, protocols, ports, and services and provide documentation describing any changes. The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed. The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput for field communications when connected during the SAT. The Vendor shall verify that SAT procedures include validation and documentation of the requirements. The Vendor shall test and install all validated
11. PHYSICAL SECURITY	Physical security must be taken into account for a total security posture. The physical perimeter access section is the traditional “gates, guns, and guards” of physical security.				
11.1 Physical Access of Cyber Components	Control system networks and devices require protection from physical access as well as cyber access.	Yes	The Vendor shall verify and provide documentation that physical security components (e.g., hardened devices, locks) are tested and the results provided. The Vendor shall disable by hardware and software means all unused ports and input/output devices (see Section 2). The Vendor shall verify and provide documentation on the two-factor authentication requiring physical access control.	Yes	The Vendor shall provide, as a part of the SAT procedures, validation and documentation of any electronic or networked room or area access devices. The Vendor shall disable by hardware and software means all unused ports and input/output devices. The Vendor shall verify and provide documentation that physical security access schemes are tested and the results provided.

11.2 Physical Perimeter Access	Perimeter security includes, but is not limited to fences, walls, fully enclosed buildings, entrance gates or doors, vehicle barriers, lighting, landscaping, surveillance systems, alarm systems, and guards. Physical security may also include site entry and exit logging as well as room or area logging possibly through a keycard access system.	Yes	The Vendor shall test and provide documentation that all alarm systems pick up all instances of intrusion with minimal false alarms.	Yes	The Vendor shall provide access control mechanisms to the Purchaser. The Vendor shall provide a walk-through of expected physical security functionality to the Purchaser. The Vendor shall provide adequate onsite training to operators and guards prior to site startup. The Vendor shall verify and provide documentation on all remote alarm, surveillance, and locking functionality prior to startup.
11.3 Manual Override Control	Manual override controls include mechanisms such as circuit breaker hand switches, valve levers, and end-device panels.	Yes	The Vendor shall verify and provide documentation that the manual control mechanism (MCM) meets the requirements appropriate for the environment in which it is deployed.	Yes	The Vendor shall verify and provide documentation that the implemented security does not compromise the required functionality of the MCM. The Vendor shall provide results of security measure assessments identifying any potential bypass vulnerabilities.
11.4 Intraperimeter Communications	Mechanisms within the perimeter may rely on intraperimeter communication to ensure secure operation. The communication medium may consist of a physical, electrical (fly-by-wire), or wireless connection.	Yes	The Vendor shall verify and provide documentation that the range of the wireless communications is limited to the required area. The Vendor shall verify and provide documentation that the physical intrusion of communication channels is detectable.	Yes	The Vendor shall verify and provide documentation that the range of the wireless communications is limited to within the perimeter. The Vendor shall verify and provide documentation that the physical intrusion of communication channels is detectable. The Vendor shall document the communication channels' locations and access points.
12. NETWORK PARTITIONING	Network partitioning refers to dividing a networked system into multiple segments to facilitate better security controls.				

12.1 Network Devices	Network devices are used to allow communication between other networked devices and networks.	Yes	The Vendor shall validate the method for managing the network devices and changing network addresses. The Vendor shall verify security levels and provide documentation of the network configuration management interface. The Vendor shall verify the ACLs, port security address lists, and describe the enhanced security for the port mirroring. The Vendor shall scan the network ports and document traffic origination and functions for each port. The Vendor shall provide documentation of firewall rules and IDS rules. The Vendor shall verify and provide documentation of the log review tools validating IDS and firewall functions. The Vendor shall verify and provide documentation of the NIPS architecture validating operations with normal and emergency control system communications. The Vendor shall verify and provide documentation of the VPN architecture filters and port security. The Vendor shall provide upgrades and patches to maintain the established level of system security.	Yes	The Vendor shall validate the method for managing the network devices and changing network addresses. The Vendor shall verify security levels and provide documentation of the network configuration management interface. The Vendor shall verify and provide documentation of the ACLs, port security address lists, and describe the enhanced security for the port mirroring. The Vendor shall scan the network ports and document traffic origination and functions for each port. The Vendor shall verify and provide documentation of firewall rules and IDS rules. The Vendor shall verify and provide documentation of the log review tools validating IDS and firewall functions. The Vendor shall verify and provide documentation of the NIPS architecture validating operations with normal and emergency control system communications. The Vendor shall verify and provide documentation of the VPN architecture verifying filters and port security. The Vendor shall provide upgrades and patches to maintain the established level of system security.

12.2 Network Architecture	Network architecture is how a network is designed and segmented into logical smaller functional subnetworks (subnets).	Yes	The Vendor shall validate and provide documentation that the higher security zones originate communication to less secure zones. The Vendor shall document all communication paths, including filtering, monitoring, and staging zones. The Vendor shall verify and provide documentation of disconnection points between the network partitions and validate the continuity of limited operations. The Vendor shall verify and provide documentation of tailored filtering and monitoring rules for all security zones and validate alarms for unexpected traffic. The Vendor shall verify and provide documentation of restricted communications through the DMZ and verify that all traffic is monitored, alarmed, and filtered. The Vendor shall verify and provide documentation of outbound filtering and alarms for unexpected traffic through security zones. The Vendor shall verify and provide documentation of all sources and destinations with enforced communication origination even during restart conditions between security zones. The Vendor shall verify and provide documentation of dual DMZ architectures using different products performing the same functionality running in parallel. The Vendor shall verify and provide documentation of a mechanism for patching a single DMZ architecture running in a parallel configuration without disruption to the	Yes	The Vendor shall validate and provide documentation that the higher security zones originate communication to less secure zones. The Vendor shall document all communication paths, including filtering, monitoring, and staging zones. The Vendor shall verify and provide documentation of test disconnection points between the network partitions and validate the continuity of limited operations. The Vendor shall test and provide documentation of tailored filtering and monitoring rules for all security zones and validate alarms for unexpected traffic. The Vendor shall validate and provide documentation of restricted communications through the DMZ and verify that all traffic is monitored, alarmed, and filtered. The Vendor shall validate and provide documentation of outbound filtering and alarms for unexpected traffic through security zones. The Vendor shall validate and provide documentation of all sources and destinations with enforced communication origination even during restart conditions between security zones. The Vendor shall validate and provide documentation of dual DMZ architectures using different products performing the same functionality running in parallel. The Vendor shall validate
13. WIRELESS TECHNOLOGIES	Wireless technologies refer to any technology, such as radio, microwave, or infrared waves, which allows analog and digital communication without the use of wires.				

13.1 Bluetooth Technology	Bluetooth technology is a short-range, wireless communications technology that can simultaneously handle both data and voice transmissions. This allows it to be used for both hands-free voice calls and data applications such as printing and synchronizing laptops, PDAs, or other mobile devices. Bluetooth technology allows Bluetooth-enabled electronic devices to connect and communicate wirelessly with a limited number of other similar devices, within proximity, as they dynamically enter and leave radio proximity.	Yes	The FAT shall be performed per written procedures agreed upon by the Purchaser. For Vendor-supplied Bluetooth-enabled device, the Vendor shall install the device and run it continuously during the entire FAT process. The Vendor shall ensure that FAT procedures include exercising all functionality and examining the input or output, and validating the results. The Vendor will specify when the results are achieved at peak performance or are environment dependent. The Vendor shall ensure that FAT procedures include written validation and documentation of each requirement.	Yes	The Purchaser shall perform the SAT testing in accordance with Vendor-supplied procedures. The Purchaser shall change any Vendor-configured or manufacturer default usernames, passwords, or other security codes at this time. The Vendor shall ensure that SAT procedures include written validation and documentation of this requirement.
13.2 Wireless Closed-Circuit TV Technology	Wireless closed-circuit TV (WCCTV) is a technology that uses video cameras and wirelessly transmits a visual signal to a specific, limited set of monitors. WCCTV is often used for surveillance in areas that need monitoring.	Yes	The FAT shall be performed per written procedures agreed upon by the Purchaser. The Vendor shall ensure that the systems have had a minimum of a 48-hour burn-in. The Vendor shall perform an interference rejection test and supply the results with an explanation of the results. The Vendor shall ensure that FAT procedures include exercising all functionality and examining the input and output, and validating the results. The Vendor shall verify compatibility of the WCCTV with other devices with which the device must interface.	Yes	The Purchaser shall perform the SAT testing in accordance with Vendor-supplied procedures. The Purchaser shall change any Vendor-configured or manufacturer default usernames, passwords, or other security codes at this time. The Vendor shall ensure that SAT procedures include written validation and documentation of this requirement. The SAT shall verify that the installed system meets the specified requirements.
13.3 Radio Frequency Identification Technology	Radio frequency identification (RFID) describes the use of radio frequency signals to provide automatic identification and tracking of items. RFID is a method of identifying and/or tracking an item (equipment, device, or other physical object) by remotely receiving information stored in a tag on the object.	Yes	The FAT shall be performed according to written procedures agreed upon by the Purchaser. The Vendor shall ensure that the systems have had a minimum of a 48-hour burn-in. The Vendor shall perform an interference rejection test and supply the results with an explanation of the results. The Vendor shall ensure that FAT procedures include exercising all functionality and examining the input or output, and validating the results. The Vendor shall verify compatibility of the RFID system with other devices with which the device must interface.	Yes	The Purchaser shall perform the SAT testing in accordance with Vendor-supplied procedures. Any Vendor-configured or manufacturer default usernames, passwords, or other security codes shall be changed at this time. The SAT shall verify that the installed system meets the specified requirements.

13.4 802.11 Technology	The reference, 802.11, refers to a family of specifications developed by IEEE for wireless local area network (WLAN) technology. It specifies a wireless interface between a wireless device and a base station (access point) or between two wireless devices (peer to peer). 802.11 devices operate in the 5 GHz and 2.4 GHz public spectrum bands. Because these transmissions are through the air, these can be intercepted or interfered with by those having the proper equipment.	Yes	The FAT shall be performed per written procedures agreed upon by the Purchaser and in agreement with the requirements of the specified sections of 802.11. For Vendor-supplied WiFi device, the Vendor shall install the device and run it continuously during the entire FAT process. The Vendor shall ensure that the systems have had a minimum of a 48-hour burn-in. The Vendor shall perform an interference rejection test and supply the results with an explanation of the results. The Vendor shall ensure that FAT procedures include exercising all functionality examining the input or output, and validating the results. The Vendor shall verify compatibility of the WiFi device with other interfaced devices.	Yes	The Purchaser shall run the 802.11 system during the entire SAT process. SAT procedures shall include exercising this functionality, examining the log files, and validating the results. Any Vendor-configured or manufacturer default usernames, passwords, or other security codes must be changed at this time. The Vendor shall ensure that SAT procedures include written validation and documentation of this requirement. The Purchaser shall perform the SAT testing in accordance with Vendor-supplied procedures. The SAT shall verify that the installed system meets the specified requirements. The Purchaser shall perform testing to: analyze the potential for radio frequency interference, determine adequate wireless LAN coverage, and set configuration parameters properly.
13.5 ZigBee Technology	ZigBee is a specification for a communication protocol using small, low-power digital radios based on IEEE 802.15.4 standard. It is more specifically known as Low-Rate Wireless Personal Area Networks (LR-WPAN) the name for a short-range, low-power, low-cost, low data-rate wireless multi-hop networking technology standard. Because these transmissions are through the air, these can be intercepted or interfered with by those having the proper equipment.	Yes	The FAT shall be performed according to written procedures agreed upon by the Purchaser and in agreement with the requirements of the ZigBee specification. For Vendor-supplied ZigBee Network or Vendor-provided ZigBee Network configuration(s), the Vendor shall install the ZigBee Network or the configuration(s) and run the ZigBee Network continuously during the entire FAT process. The Vendor shall ensure that FAT procedures include exercising this functionality, examining the log files, and validating the results. The Vendor shall ensure that the systems have had a minimum of a 48-hour burn-in. The Vendor shall perform an interference rejection test and supply the results with an explanation of the results. The Vendor shall verify compatibility of the LR-WPAN device with other devices with which the device must interface.	Yes	The Purchaser shall run the ZigBee Network during the entire SAT process. SAT procedures shall include exercising this functionality, examining the log files, and validating the results. The Purchaser shall change any Vendor-configured or manufacturer default usernames, passwords, or other security codes at this time. The Vendor shall ensure that SAT procedures include written validation and documentation of this requirement.

13.6 WirelessHART Technology	Wireless Highway Addressable Remote Transducer (HART) is a Wireless Mesh Network Communications Protocol designed to meet the needs of process automation applications. WirelessHART is a key part of the HART Field Communications Protocol Revision 7 and is backward compatible with existing HART devices and applications. The WirelessHART standard was approved on June 2007 and was released in September 2007. WirelessHART is in the early stages of development and deployment; hence, there is not much publicly available information regarding its security. It shall be noted that because the IEEE 802.15.4 protocol is the basis for this technology, the previous IEEE 802.15.4 security analysis is applicable. WirelessHART like all wireless technologies is subject to the same security issues because of over the air	Yes	The FAT shall be performed per written procedures agreed upon by the Purchaser and in agreement with the requirements of the WirelessHART specification. For Vendor-supplied WirelessHART Network or Vendor-provided WirelessHART Network configuration(s), the Vendor shall install the WirelessHART Network or the configuration(s) and run the WirelessHART Network continuously during the entire FAT process. The Vendor shall ensure that FAT procedures include exercising this functionality, examining the log files, and validating the results. The Vendor shall ensure that the systems have had a minimum of a 48-hour burn-in. The Vendor shall perform an interference rejection test and supply the results with an explanation of the results. The Vendor shall verify compatibility of the WirelessHART device with other devices with which the device must interface.	Yes	The Purchaser shall run the WirelessHART Network during the entire SAT process. SAT procedures shall include exercising this functionality, examining the log files, and validating the results. The Purchaser shall change any Vendor-configured or manufacturer default usernames, passwords, or other security codes at this time. The Vendor shall ensure that SAT procedures include written validation and documentation of this requirement.
13.7 Mobile Radios	Mobile radios refer to wireless communications systems and devices that transmit and receive information, primarily voice, on radio frequencies. The transmitter and/or the receiver are mobile. Because these devices transmit wirelessly, these are subject to interception and modification of the signals.	Yes	The FAT shall be performed per written procedures agreed upon by the Purchaser. The Vendor shall ensure that the systems have had a minimum of a 48-hour burn-in. The Vendor shall perform an interference rejection test and supply the results with an explanation of the results. The Vendor shall ensure that FAT procedures include exercising all functionality and examining the input or output, and validating the results. The Vendor shall verify compatibility of the mobile radio with other wireless devices with which the device must interface. The Vendor shall ensure that FAT procedures include written validation and documentation of this requirement.	Yes	The Purchaser shall perform the SAT testing in accordance with Vendor-supplied procedures. The Purchaser shall change any Vendor-configured or manufacturer default usernames, passwords, or other security codes at this time. The Vendor shall ensure that SAT procedures include written validation and documentation of this requirement. The SAT shall verify that the installed system meets the specified requirements.

13.8 Wireless Mesh Network Technology	A Wireless Mesh Network (WMN) is a communications network made up of radio nodes organized in a mesh topology. In WMNs, nodes are composed of mesh routers and mesh clients. Each node operates not only as a host but also as a router, forwarding packets on behalf of other nodes that may not be within direct wireless transmission range of their destinations. Potential vulnerabilities exist with route management protocols, remote centralized management system, and over-the-air firmware upgrades via IP Internet traffic, WMN operating system, and applications running on any node of the wireless mesh network such as SSH (Secure Shell) daemons or lightweight Hypertext Transfer Protocol (HTTP) servers. Because the transmissions between WMN nodes are through the air, they can be intercepted or interfered	Yes	The FAT shall be performed per written procedures agreed upon by the Purchaser and in agreement with the requirements of the specified sections of 802.11. For Vendor-supplied WiFi device, the Vendor shall install the device and run it continuously during the entire FAT process. The Vendor shall ensure that the systems have had a minimum of a 48-hour burn-in. The Vendor shall perform an interference rejection test and supply the results with an explanation of the results. The Vendor shall ensure that FAT procedures include exercising all functionality and examining the input or output, and validating the results. The Vendor shall verify compatibility of the WiFi device with other interfaced devices.	Yes	The Purchaser shall run the 802.11 system during the entire SAT process. SAT procedures shall include exercising this functionality, examining the log files, and validating the results. Any Vendor-configured or manufacturer default usernames, passwords, or other security codes must be changed at this time. The Vendor shall ensure that SAT procedures include written validation and documentation of this requirement. The Purchaser shall perform the SAT testing in accordance with Vendor-supplied procedures. The SAT shall verify that the installed system meets the specified requirements. The Purchaser shall perform testing to: analyze the potential for radio frequency interference, determine adequate wireless WMN coverage, and set configuration parameters properly.
13.9 Cellular Technology	Monitoring and controlling equipment occurs at various points within an enterprise. In many cases, traditional cabled solutions or private radio networks are not a cost-effective option to cover all assets. Cellular technology may be used to manage and control industrial processes where cabling is not an option. Although the law provides penalties for the interception of cellular telephone calls, it is easily accomplished and impossible to detect.	Yes	The FAT shall be performed per written procedures agreed upon by the Purchaser. The Vendor shall ensure that the systems have had a minimum of a 48-hour burn-in. The Vendor shall perform an interference rejection test and supply the results with an explanation of the results. The Vendor shall ensure that FAT procedures include exercising all functionality and examining the input or output, and validating the results. The Vendor shall verify compatibility of the cellular system with other devices with which the system must interface.	Yes	The Purchaser shall perform the SAT testing in accordance with Vendor-supplied procedures. The Purchaser shall change any Vendor-configured or manufacturer default usernames, passwords, or other security codes at this time. The Vendor shall ensure that SAT procedures include written validation and documentation of this requirement. The SAT shall verify that the installed system meets the specified requirements.

13.10 WiMAX Technology	WiMAX is the name given to the IEEE 802.16 standards. While similar to WiFi, WiMAX is very different. WiMAX is a long-range system. WiFi is a short-range system. WiMAX has a QoS implementation that is different from WI-Fi and its MAC layer uses a scheduling algorithm, while WiFi is based on a contentions access system (i.e., Carrier Sense Multiple Access). But, because these transmissions are through the air like WiFi, they can be intercepted or interfered with by those having the proper equipment. WiMAX is a wireless broadband technology made for longer distances based on the IEEE 802.16 standard. WiMAX is a relatively new technology that can be configured for point-to-point links, point-tomultipoint links or mobile cellular type access. WiMAX uses both licensed and unlicensed frequencies: 2.3–2.7, 3.4–3.6, and 5.8 GHz bands . Like other	Yes	The FAT shall be performed per written procedures agreed upon by the Purchaser. The Vendor shall ensure that the systems have had a minimum of a 48-hour burn-in. The Vendor shall perform an interference rejection test and supply the results with an explanation of the results. The Vendor shall ensure that FAT procedures include exercising all functionality and examining the input or output, and validating the results. The Vendor shall verify compatibility of the WiMAX equipment and communications with other devices with which the device must interface.	Yes	The Purchaser shall perform the SAT testing in accordance with Vendor-supplied procedures. The Purchaser shall change any Vendor-configured or manufacturer default usernames, passwords, or other security codes at this time. The Vendor shall ensure that SAT procedures include written validation and documentation of this requirement. The SAT shall verify that the installed system meets the specified requirements.

13.11 Microwave and Satellite Technology	Both microwave and satellite communications use microwaves for transmitting information from point to point, both fixed and mobile. Point-to-point communication is directly between two points on the earth and requires unobstructed LoS. This is typical in a microwave communication link between two cellular network towers. Point-to-multipoint communication provides coverage from a single tower, which may include both LoS and non-LoS paths. Satellite communications transmit from a point on the earth to a satellite and then back to other points on the earth. Satellites introduce some potential latency but can transmit over longer distances and provide connectivity in very remote areas. Microwave communications are preferable because satellite technology is the more expensive technology. Both microwave and satellite transmissions are susceptible to	Yes	The FAT shall be performed per written procedures agreed upon by the Purchaser and in agreement with the requirements of GR-63 NEBS and GR-1089. For Vendor-supplied microwave device, the Vendor shall install the device and run it continuously during the entire FAT process. The Vendor shall ensure that the systems have had a minimum of a 48-hour radio/gear burn-in. The Vendor shall also apply a bit error test for a minimum of 24 hours and verify that it has the agreed upon level of accuracy. The Vendor shall perform an interference rejection test and supply the results with an explanation of the results. The Vendor shall ensure that FAT procedures include exercising all functionality and examining the input or output, and validating the results. The Vendor shall ensure that FAT procedures include written validation and documentation of this requirement.	Yes	The Purchaser shall perform the SAT testing in accordance with Vendor-supplied procedures. Any Vendor-configured or manufacturer default usernames, passwords, or other security codes must be changed at this time. The Vendor shall ensure that SAT procedures include written validation and documentation of this requirement. The SAT shall verify that the installed system meets the specified requirements.