DIVISION 25: INTEGRATED AUTOMATION

SECTION 25 00 00: GENERAL REQUIREMENTS FOR INTEGRATED AUTOMATION

PART 1 - GENERAL

1.1 **SUMMARY**

A. This section includes general requirements for Integrated Automation systems, specifically focusing on:

1. Operational Technology (OT) Cyber Security
2. Remote Access for OT
3. OT Network Management
4. Secure Encrypted Cloud Connections

B. The requirements in this section apply to all related sections of Division 25.

1.2 **REFERENCES**

A. Comply with applicable standards and guidelines, including but not limited to:

1. National Institute of Standards and Technology (NIST)
2. International Society of Automation (ISA)
3. ISO/IEC 27001:2013 Information Security Management
4. SOC 2 Type 2 Certification

1.3 **SUBMITTALS**

A. Submit the following for approval:

1. OT Cyber Security Plan
2. Remote Access Configuration and Security Plan
3. OT Network Management Plan
4. Secure Encrypted Cloud Connection Plan
5. Product Data Sheets from Secure Edge and Cloud Platform
6. Certifications and Compliance Statements
7. Audit and Incident Reporting Plan

1.4 **QUALITY ASSURANCE**

A. Engage qualified personnel with demonstrated experience in OT cyber security, remote access configuration, and network management.

B. Ensure all systems and components comply with applicable regulatory requirements and industry standards.

PART 2 - PRODUCTS

2.1 **OPERATIONAL TECHNOLOGY (OT) CYBER SECURITY**

A. Provide an OT cyber security solution, such as Neeve Secure Edge, that includes, but is not limited to:

1. Network segmentation and segregation
2. Zero-Trust network architecture
3. Intrusion detection and prevention systems (IDS/IPS)
4. Firewalls and secure gateways
5. Endpoint protection and antivirus software
6. Patch management and vulnerability assessment tools
7. Security information and event management (SIEM) system
8. User authentication and access control mechanisms with MFA
9. Secure Edge Professional gateway with hardware security (TPM2.0)

B. Features should include:

1. High capacity for supporting multiple LANs and edge applications.
2. Security policy management & monitoring.
3. Threat detection & alerting.
4. Support for high-availability and edge-clustering configurations.

2.2 **REMOTE ACCESS FOR OT**

A. Implement secure remote access solutions, such as those provided by Neeve Secure Edge Cloud Platform, that include:

1. Zero trust network architecture (ZTNA) best practices
2. Role-based access control (RBAC)
3. Unlimited remote access sessions.
4. Support for NIST least-privilege model of access and management
5. Logging and monitoring of remote access sessions
6. Agentless web-based remote access devices and applications
7. Secure Sockets Layer (SSL) protocols with book-ended architecture and x509v3 certificates
8. Encryption of data at rest and in transit

B. Provide remote access portals for managing users, policies, and devices, including:

1. RDP, SSH, HTTP, HTTPS, TELNET, VNC and TCP / UDP access
2. Granular access control to the device and port level

3. Multiple levels of administration supporting NIST list-privilege
4. Scheduled access for time-based control
5. Single Sign On (SSO) & Multi-Factor Authentication (MFA) support

2.3 **OT NETWORK MANAGEMENT**

A. Provide network management tools and systems, such as Neeve Secure Edge Cloud Platform, that include:

1. Network monitoring and management software
2. Configuration management and backup solutions
3. Performance monitoring and analytics
4. Incident response and management capabilities
5. Network access control (NAC)
6. Automated network discovery and mapping

B. Features should include:

1. Enablement of Zero trust network architecture (ZTNA) best practices
2. End-point device discovery and monitoring
3. Network segmentation and management
4. 802.1x based authentication support
5. Support for WAN and LAN failover

2.4 **SECURE ENCRYPTED CLOUD CONNECTIONS**

A. Provide solutions for secure encrypted cloud connections, such as Neeve Secure Edge Cloud Platform, that include:

1. End-to-end encryption for data in transit between edge devices and cloud services.
2. Secure SDWAN with integrated encryption.
3. Support for major cloud providers such as AWS, Azure, VMware, GCP, and OpenStack.
4. Book-ended architecture using x509v3 certificates for authentication and encryption.
5. Capabilities for connecting building systems to the cloud for data streaming and cloud-based control.

B. Features should include:

1. Unlimited connections and tunnels included in the license.
2. Centralized management and configuration of cloud connections.
3. Secure cloud connectivity with a zero trust approach.
4. Monitoring and logging of all cloud connection activities for compliance and security.

PART 3 - EXECUTION

3.1 **INSTALLATION**

A. Install all systems and components in accordance with manufacturer instructions and industry best practices.

B. Ensure proper configuration and integration of all components to achieve a secure and efficient OT environment.

C. All connections between building automation systems and the public internet go through the Secure Edge device. No third party VPN connections are allowed.

3.2 **TESTING AND COMMISSIONING**

A. Perform comprehensive testing of all OT cyber security measures, remote access configurations, network management systems, and secure cloud connections.

B. Document all test results and obtain approval before moving to full operation.

3.3 **TRAINING**

A. Provide training for relevant personnel on the operation and management of OT cyber security, remote access, network management systems, and secure cloud connections.

B. Ensure training includes practical exercises and scenarios to ensure readiness for real-world operations.

3.4 **MAINTENANCE AND SUPPORT**

A. Provide ongoing maintenance and support services for all installed systems.

B. Ensure regular updates and patches are applied to maintain security and performance.

C. Support levels:

1. **Basic**: Email and web support, 8 hours/5 days availability, 1-week hardware replacement.
2. **Professional**: Email, web, and phone support, 24 hours/7 days availability, 1 business day hardware replacement.
3. **Enterprise**: Enhanced support as per Professional with additional features.