Purchase Description: Most current Lenel on guard Access control System that is HSPD-12 and FIPS complainant and accepts Common Access Cards

Product Line: Lenel OnGuard Access control System

Deployment Type: On-premise

Scope: Comprehensive physical access control and integrated security management solution for Irwin Army Community Hospital, Fort Riley KS 66442.

System Overview:

The OnGuard platform is a scalable, open-architecture access control system designed to unify access control with alarm integration for organizations.

Key Features & Capabilities:

Access Control: Unlimited card readers, alarm points, and cardholders; supports multiple card formats, biometric integration, and mobile credentials.

Integration: Bi-directional exchange with HR, ERP, elevator systems; coordination with emergency response and building management systems

Hardware: Intelligent System Controllers (ISCs), Lenel-branded and HID readers, card printers, and optional biometric devices.

Network: Ethernet, RS-232/485, dual-path communications; FIPS 197 128-bit AES encryption

Scalability: Supports growth from current needs to future expansion without major redesign

Technical product training, software upgrades, and support plans

Professional Engineering Services (PES) for installation and integration

Implement OnGuard to secure entry points, and provide remote access control via mobile devices for a hybrid workforce.

1. General Overview & Scope

This document outlines the technical, operational, and functional requirements for the procurement, installation, and integration of a comprehensive physical access control and integrated security management solution.

- Location: Irwin Army Community Hospital, Fort Riley, KS 66442.
- Deployment Type: On-premise.
- Target Product Line: Most current version of the Lenel OnGuard Access Control System
- Core Objective: Implement a scalable, open-architecture access control system to secure facility entry points, unify access control with alarm integration, and provide remote access control via mobile devices for a hybrid workforce.

2. Compliance & Security Standards

To ensure compatibility with Department of Defense (DoD) and federal security mandates, the proposed solution MUST meet the following compliance requirements:

- HSPD-12 Compliance: Fully compliant with Homeland Security Presidential Directive 12.
- FIPS Compliance: Must meet Federal Information Processing Standards, specifically utilizing FIPS 197 128-bit AES encryption for all network communications. FIPS 201
- Credential Compatibility: Must natively accept and process standard issue Common Access Cards (CAC).

3. Key Features & Operational Capabilities

The platform must provide a unified security management environment with the following functional capabilities:

Category	Required Capabilities
Capacity	Must support an unlimited number of card readers, alarm points, and cardholders to prevent future licensing bottlenecks.
Credentials	Must support multiple card formats, seamless biometric integration, and mobile credentials for remote access control.

Integration	Must support bi-directional data exchange with HR and ERP systems. Must coordinate and interface with elevator systems, emergency response platforms, and broader building management systems.
Scalability	Must architecturally support organizational growth—from current baseline needs to future expansions—without requiring major system redesign or forklift upgrades.

4. Hardware & Network Specifications

The vendor shall provide and integrate all necessary hardware and network components, including but not limited to:

- Controllers: Intelligent System Controllers (ISCs) capable of localized decision-making.
- Peripherals: Lenel-branded and HID-compatible card readers, identification card printers, and optional biometric capture devices as designated.
- Network Communications: Must support Ethernet, RS-232, and RS-485 protocols, utilizing dual-path communications for redundancy and high availability.

5. Professional Services, Training, & Support

The procurement package must include comprehensive lifecycle support to ensure successful deployment and sustainment:

- Professional Engineering Services (PES): Full installation, configuration, and integration of the OnGuard system into the existing Irwin Army Community Hospital infrastructure.
- Training: Technical product training for system administrators and security operators.
- Sustainment: Provision of software upgrade protection and ongoing technical support plans.