**Created:** 2025-10-29 **Updated from:** Pryor\_Bod\_EVS\_Rev01.md

# BASIS OF DESIGN - ELECTRONIC SAFETY AND SECURITY

## CSI Division 28

### Pryor Data Center - PACHYDERM GLOBAL

**Parent Document:** [[Saga Pryor DC/Basis of Design/Erik\_BOD\_Updated/\_BOD - Exec Summary and TOC]]

## OVERVIEW

Multi-layered physical security system protects personnel, IT equipment, and facility infrastructure through defense-in-depth security zoning, access control, video surveillance, and intrusion detection integrated with BMS/DCIM for centralized monitoring.

**Design Philosophy:** - **Layered defense model:** Security zones with progressive access controls (CP 1 through CP 5) - **ISO 27001:2022 alignment:** Physical security controls support Information Security Management System (ISMS) - **Integration:** All systems monitored from Security Control Room (SCR) with 99.982% availability target - **Compliance:** SOC 2 Type II, ISO 27001, PCI DSS physical security requirements - **Life safety priority:** Security systems override on fire alarm (egress first)

## SECURITY ZONE FRAMEWORK

The data center is divided into distinct security zones creating a layered defense model with specific Control Points (CP) that correspond to progressive security challenges. Each zone transition as a normal means of access requires access control. Emergency egress doors are alarmed.

### Security Zone Definitions

| Zone Color | Control Point | Definition & Access Requirements |
| --- | --- | --- |
| **Violet** | CP 1 | Inside perimeter fence but outside building envelope. Includes parking lots, equipment yards, generator areas. **Access:** Perimeter gates with card reader/intercom |
| **Blue** | CP 2 | Visitor reception areas inside building but outside private offices and critical areas. Includes security vestibule lobbies, designated conference rooms/restrooms. **Access:** Building entry mantrap with card reader |
| **Yellow** | CP 3 | Access-controlled private office areas for customers and PACHYDERM personnel. **Access:** Card reader from Blue Zone |
| **Orange** | CP 4 | Secure data center premises restricted to authorized personnel with special access clearance. Includes data halls (DH1, DH2). **Access:** Card + biometric (MFA) via CICO checkpoint |
| **Red** | CP 5 | Most critical spaces protecting essential operations. Includes electrical rooms (PDMs, transformers), mechanical rooms (chillers, pumps), SCR, network rooms (MDF/IDF). **Access:** Card + biometric (MFA), highest clearance |
| **Black** | N/A | Construction zones not yet operational, physically separated from active areas. **Access:** Dedicated construction access, temporary barriers |

### Risk Level Classification

SAGA assesses threat level for each site. The Pryor Data Center is classified as **High Risk (HR)** due to: - Critical infrastructure role in data center operations - Tornado Alley location requiring enhanced physical protection - High-value IT assets and sensitive customer data

**Risk Level Requirements Summary:**

| Requirement | Medium Risk (MR) | High Risk (HR) - **Pryor DC** |
| --- | --- | --- |
| **Perimeter Berm** | Not required | **Required** |
| **Perimeter Lighting** | Reactive (motion) | **Persistent (always on)** |
| **Main Vehicle Entrance** | K4-rated arrestor | **Sally Port with K4** |
| **Pedestrian Entrances** | Standard gate | **Full-height turnstiles** |
| **Fence-to-Building Standoff** | 45 ft (15 m) min | **100 ft (30 m) min** |
| **Permanent Visitor Center** | Not required | **Required at gate** |
| **Exterior Orange Zone Doors** | Standard | **15-min forced entry resistance** |
| **SCR Transaction Window** | 4×6 in. opening | **Solid with transaction drawer** |
| **Roof Surveillance** | Inside doors only | **Inside + outside with thermal** |

### Foundational Security Tenets

**System Resilience & High Availability:** - Electronic security systems classified as critical infrastructure - **Availability KPI:** 99.982% uptime per annum (aligned with Tier III) - Redundant components and high-availability architectures (see Section 8.2)

**Infrastructure Integrity:** - Security systems protected from physical and cyber-physical attack - All field devices, cabling, and network infrastructure hardened (see Section 3.12) - Tamper-proof enclosures with integrated tamper switches

**Personnel Accountability:** - Access granted based on least privilege principle - Formal security clearance process (Levels 1-5, see Section 3.9) - Granting, review, and revocation strictly controlled

## GENERAL SECURITY REQUIREMENTS (ALL ZONES)

### Zone Transition and Door Controls

**Access Control Doors:** - Any pathway transitioning between zones as a normal means of access must be access-controlled - Standard equipment per door: - Card reader on non-hinge side (exterior and interior) - Recessed door contact per door leaf - Electric mortise security lock with bolt position sensor - Wire distributor box or device junction box - Intercom (required on: main/rear entrances, penthouse doors, pedestrian/vehicle gates, bypass doors)

**Emergency Egress Doors:** - Doors for life safety code not used for normal access - Equipment: - Recessed door contact per door leaf - Door horn and strobe (centrally mounted above door) for door-forced-open alerts - AHJ-approved exit device - No exterior handles/levers/grips (where AHJ permits)

**Video Surveillance:** - Cameras required on interior and exterior of every access-controlled or supervised door - Each camera dedicated to the door it covers - Sufficient resolution to identify personnel

### Multi-Factor Authentication (MFA) & Biometric Requirements

To enhance security beyond card-based access, MFA is required at high-risk transitions combining “something you have” (access card) with “something you are” (biometric).

**Mandatory Biometric Authentication Points:** - All transitions from Blue Zone (CP 2) to Orange Zone (CP 4) - All transitions to Red Zone (CP 5) - Inner door of all mantraps - Dedicated data hall access doors

**Approved Biometric Modalities:** - **Primary:** Iris recognition, fingerprint (FAP 45+ quality), palmprint, or facial recognition - **Facial Recognition:** ISO/IEC 19794-5 compliant, False Acceptance Rate (FAR) <0.001% - **Template Storage:** Encrypted format, non-extractable from system

**Enrollment and Management:** - Enrollment conducted in supervised secure environment by authorized security personnel - Prompt revocation upon employment/contract termination

## VIOLET ZONE (CP 1) - PERIMETER SECURITY

### Perimeter Barrier & Standoff

**Fencing:** - **Type:** 8 ft (2.4 m) tall anti-scale, rigid, forced-entry/crash-rated fence - **Material:** Galvanized steel, 9-gauge wire, 2” mesh (or anti-climb mesh) - **Anti-Dig Barrier:** Concrete barrier 12 in. (300 mm) width × 18 in. (457 mm) depth along fence base - **Standoff Distance:** **100 ft (30 m) minimum** from fence to building (HR site requirement) - **Clear Zone:** Standoff area kept clear of obstructions aiding climbing or providing concealment - **Lighting:** **Persistent (always on)** at 5 lux along fence line, 30 lux at gate entrances (HR requirement)

**Perimeter Berm (HR Requirement):** - Earthen berm surrounding perimeter for additional vehicle barrier - Integration with site grading and stormwater management

### Vehicle Entrances

**Two Property Entrances:**

**1. Main Entrance (NE Corner):** - **Configuration:** Full sally port (interlocking dual-gate system) with vehicle trap for main entrance - **Location:** NE corner of property - **Staffing:** Permanent manned visitor center (HR requirement) - **Usage:** Primary entrance for all normal operations, deliveries, visitors, and personnel - **Sized for:** Largest anticipated delivery trucks - **K4-rated vehicle arrestor:** 15,000 lb vehicle at 30 mph - **Rejection lane:** For vehicles turned away without entering secure perimeter

**Access Control:** - Access control pedestals with card readers located minimum 15 ft (4.5 m) from gate - Video intercom on both sides - Integration with Security Control Room (SCR) for remote verification - Vehicle loop detectors

**Permanent Visitor Center (HR Requirement):** - Climate-controlled guard post at main gate - Equipped with: - Duress alarms - Communications equipment - Direct control of sally port gates - Government ID verification capability - Initial vehicle/personnel screening station

**2. Secondary Entrance (NW Corner - Emergency/Construction Access):** - **Configuration:** Single-gate with K4-rated vehicle arrestor - **Location:** NW side of property - **Staffing:** Normally unmanned - **Usage:** Emergency access, special construction activities, maintenance operations (not employed during normal operations) - **Visibility:** Gate visible from Security Control Booth (SCB) located at loading dock - **Surveillance:** CCTV coverage integrated with SCB and SCR monitoring

**Access Control (Secondary Entrance):** - Card reader and video intercom - Remote operation from SCB or SCR - Vehicle loop detectors - Log all access events - Normally secured and locked; activated only for emergencies or pre-authorized construction/maintenance activities

### Pedestrian Gates

**Main Pedestrian Entrance (NE Corner):** - **Location:** Adjacent to main vehicle sally port at NE corner - **Full-height turnstile** (HR site requirement) or card-controlled gate - Card reader and video intercom on both sides - Located minimum 15 ft from vehicular sally port for safety

**Secondary Pedestrian Access (NW Corner):** - **Location:** Adjacent to secondary emergency/construction vehicle entrance - Card-controlled gate with video intercom - Normally locked; activated only during emergency or authorized construction/maintenance operations

### Line-of-Sight Perimeter Intrusion Detection

**System Requirements:** - Line-of-sight system (microwave, infrared beam, or volumetric laser) parallel to interior of fence - Creates invisible detection curtain resistant to environmental interference (fog, rain, wind, fauna) - Zonal coverage allowing SCR to pinpoint breach location - High detection probability with minimized false alarms

**Integration and Alarm Response:** - Full integration with central security platform in SCR - Immediate audible/visual alert on alarm - Pre-programmed response protocol: - Immediate verification using nearest PTZ camera - Dispatch of roving security patrol - Activation of localized strobe/audible alarm in breach zone - All intrusion attempts logged as security events

**Perimeter CCTV:** - Fixed cameras covering all fence sections (360° coverage) - PTZ cameras at corners with preset positions - Thermal imaging for nighttime detection - Integration with intrusion detection (camera preset on alarm)

### Vehicle Barriers

**Crash-Rated Bollards:** - **Rating:** K4 (15,000 lb vehicle at 30 mph) minimum; K12 (15,000 lb at 50 mph) for highest risk areas - **Location:** - Building entry points (main entrance, loading dock) - Generator yard perimeter - 138kV substation perimeter - Critical transformer locations - **Spacing:** 4-5 ft on center (prevent vehicle passage) - **Material:** Steel-reinforced concrete or steel pipe filled with concrete - **Standards:** ASTM F2656, DOS SD-STD-02.01

## BLUE ZONE (CP 2) - LOBBIES & SECURITY VESTIBULE

### Main Building Entry

**Location:** Main entrance to building

**Configuration:** Full control glass security mantrap with double-door airlock

**Access Control:** - **Outer door:** Card reader (all authorized personnel, visitors with escort) - **Inner door:** Card reader + biometric MFA (Level 2+ clearance required) - **Interlock:** Outer must close before inner opens - **Surveillance:** CCTV cameras with 125 PPFW (Pixels Per Face Width) for positive identification - **Fire override:** Both doors unlock on fire alarm

**Mantrap Requirements:** - Single-person occupancy enforcement (sensors + visual verification) - Video recording of all authentication events - Integration with Security Control Room (SCR) for alarm response - Intercom for SCR communication on authentication failures - Delayed egress systems for tailgating deterrence

**Facilities Access:** - Main visitor waiting area (Blue Zone) - Restrooms and locker connection - Reception desk for visitor check-in

### Mantrap & Security Portal Operating Procedure

Security portals (mantraps) are critical for preventing tailgating and unauthorized entry.

**Single Person Entry Rule:** - Only one authorized person permitted within mantrap vestibule at any time - Inner door remains locked until outer door fully closed and credentials verified

**Standardized Entry Sequence:** 1. Individual presents access credential (badge) to outer door card reader 2. Upon valid read, outer door unlocks; individual enters and allows door to close completely 3. Inside mantrap, individual presents biometric authentication to inner door reader 4. Only after successful biometric verification will inner door unlock 5. If authentication fails or tailgating detected, both doors remain locked and security alarm sent to SCR 6. Individual must communicate with SCR via integrated intercom

**Egress Sequence:** 1. Motion sensor or push-to-exit button unlocks inner door from secure side 2. Individual enters mantrap; inner door closes 3. Outer door automatically unlocks for exit 4. No credential required for egress (life safety compliance)

**Video Surveillance:** - All mantraps monitored by cameras meeting ‘Critical Point Identification’ standard (125 PPFW) - Visual verification of single-person entry rule - Recording of all authentication events

### Visitor Management & Escorting Procedure

**Pre-Arrival & Check-in:** - **Pre-Authorization:** All visitors pre-registered minimum 24 hours in advance by authorized representative - **Arrival & Verification:** At Main Gatehouse (Violet Zone), visitors present government-issued photo ID verified against pre-authorization list - **Badge Issuance:** Temporary “Visitor” badge issued (time-bound, expires end of authorized visit date) - Badge must be visibly worn at all times

**Escorting Requirements:** - **General Rule:** All visitors escorted by authorized PACHYDERM or tenant host beyond Blue Zone (CP 2) - **Secure Zones:** Mandatory escorting for Yellow (CP 3), Orange (CP 4), or Red (CP 5) zone access - **Escort Responsibility:** Host responsible for visitor conduct and security protocol adherence - **Exceptions:** Pre-authorized badged vendors with work orders may access designated work area unescorted per clearance level

**Check-out & Badge Return:** - Visitor returns temporary badge at Main Gatehouse or Blue Zone security desk - Return logged to complete audit trail

## YELLOW ZONE (CP 3) - ADMINISTRATIVE & OFFICE AREAS

**General Requirements:** - Yellow Zones access-controlled and physically separated from all other zones - Access from Blue Zone (CP 2) requires card reader - Doors to all other zones (Orange, Red) secured with reader on both sides - Clear desk and clear screen policy for all workstations/workspaces - Automatic screen lock after maximum 15 minutes of inactivity

## ORANGE ZONE (CP 4) - DATA HALLS

### General Requirements

* Orange Zones have single main entrance for normal ingress/egress
* All other doors designated for specific purposes (rack movement) or emergency exits only
* Orange Zones not located on exterior building walls
* **15-minute forced entry resistance rating** for all exterior doors (HR site requirement)

### Clean In/Clean Out (CICO) Checkpoint

**Purpose:** Ensure no unauthorized equipment, materials, or data brought into or removed from data hall.

**Infrastructure Requirements:** - **Tailgate Prevention:** Technology required at entrance - **Screening Area:** Space for security officers to screen personnel and inspect items - Designated tables for tool/equipment examination - Storage for handheld screening devices (wands) - Full-height magnetometer - **CCTV Coverage:** Entire area including item inspection tables at ‘Critical Point Identification’ level (125 PPFW) - **Power:** All screening equipment supplied with UPS-backed power

**Asset & Tool Control Procedure:** 1. **Pre-Authorization:** All tools, equipment, and removable media pre-authorized via valid ticketed work order 2. **Entry Inspection:** Items presented to security for verification against work order 3. **Entry Logging:** Each item logged (description, serial number, individual, work order number, time) 4. **Visual Inspection:** Security inspects all tools, equipment, and containers 5. **Exit Inspection:** Mandatory presentation of all items for exit verification 6. **Exit Logging:** Exit log updated (time of departure, clearance confirmation) 7. **Prohibited Items:** Defined list enforced (personal mobile phones, cameras, unapproved wireless devices must be secured in Blue Zone lockers)

### Walls, Floors, and Ceilings

* All boundaries (walls, floors, ceilings) permanently constructed slab-to-slab
* Visual evidence of any attempted unauthorized penetration

**External Walls:** - Protected from vehicle attack via crash-rated fences, bollards, or robust wall construction - Minimum 7.75 in. (200 mm) reinforced concrete

**Internal Walls:** - Solid-panel or mesh construction - Mesh walls: minimum 10 AWG steel, no larger than ½ in. × ½ in. openings

### Video Surveillance

**Coverage Inside Data Hall:** - Main corridors and perimeter walkways - Hot and cold aisles - All alarm points and security panel locations - NOT directed into customer cages (privacy protection)

## RED ZONE (CP 5) - FACILITY & SUPPORT AREAS

### Walls and Doors

**Exterior Walls:** - **MR sites:** 5-minute penetration resistance - **HR sites (Pryor DC):** **15-minute penetration resistance**

**Exterior Doors:** - Utility and emergency exit doors kept to minimum - All normal-use doors are standard access control doors - Card + biometric (MFA) required

### Security Control Room (SCR)

**Dimensions:** - Minimum 12 ft × 24 ft (3.65 m × 7.3 m)

**Workstation Security:** - All workstations enforce clear screen policy - Automatic screen lock after maximum 15 minutes of inactivity

**Physical Security:** - Walls, doors, and transaction window meet forced-entry or ballistic resistance per risk level - **Transaction Window (HR sites):** Solid with transaction drawer (not open 4×6 in. opening) - Duress button installed inside control room

**System Redundancy and High Availability:**

To ensure continuous security monitoring aligned with Tier III availability objectives: - **Redundant Security Servers:** Surveillance servers/recorders and storage area networks (SAN) in active-active or active-passive configuration - **Redundant Network Infrastructure:** Dual switches and paths for dedicated security systems network - **Redundant Access Control Servers:** Automatic failover capabilities - **Diverse Power Sources:** All redundant components powered from different PDUs where possible - **Availability Target:** 99.982% uptime per annum

**Power:** - All security equipment (panels, racks) on emergency power (generator with UPS battery bridge) - UPS runtime: minimum 15 minutes (full load)

**Data Integrity and Retention:** - Historical security data (camera footage, access logs, IDS events) stored minimum 90 days - Redundant storage architecture ensures data integrity during failover

### Network & Security Equipment Rooms (MDF/IDF)

* Standard access control doors
* Secondary intrusion detection sensor inside room monitoring entrance
* Video surveillance covering equipment cabinets (250 pixels per meter resolution)
* Dedicated HVAC with individual temperature control
* Plywood-backed walls for equipment mounting

### Loading Dock

* CCTV coverage of all overhead/pedestrian doors, exterior dock area, interior of trailers during loading/unloading (250 pixels per meter)
* Motion detection as secondary intrusion layer covering all entrances

### Generator Yard & Rooftop

**Generator Yard:** - Access controlled by 8 ft (2.4 m) tall anti-climb fence with anti-climb topper (3 strands barbed wire) - Access doors from data center limited to maintenance requirements only - Fixed and PTZ cameras providing complete view of all generator sides - No permanent parking in critical equipment areas

**Rooftop:** - Access points (hatches, doors) hardened and equipped with access control and IDS sensors - **HR sites:** Cameras with thermal or video analytics monitor rooftop perimeter for unauthorized activity - Coverage of interior and exterior of all roof access points

## BLACK ZONE - CONSTRUCTION ZONES

**General Requirements:** - **Physical Separation:** Black Zones physically separated from all active operational areas with temporary barrier (floor-to-ceiling stud wall) - **Dedicated Access:** Construction workers use dedicated entrances and pathways that do not cross active zones - **Access Control:** Controlled via dedicated ACS or manually controlled checkpoint monitored by security personnel - **Transition:** Upon completion, construction zones transitioned to appropriate operational zone color

## PERSONNEL SECURITY CLEARANCE & ACCESS PROVISIONING

All personnel (employees, contractors, vendors) must be formally granted a security clearance level defining authorized access privileges. The granting, review, and revocation process is strictly controlled and documented.

### Security Clearance Levels

| Clearance Level | Authorized Unescorted Access | Typical Roles |
| --- | --- | --- |
| **Level 1: Escorted Visitor** | Blue Zone (CP 2) only, under constant escort | Clients, guests, temporary visitors |
| **Level 2: General Staff** | Yellow Zone (CP 3) and Blue Zone (CP 2) | PACHYDERM administrative staff, tenant office personnel |
| **Level 3: Technical Staff** | Yellow (CP 3), Blue (CP 2), designated Red Zone (CP 5) areas per role | Infrastructure engineers, maintenance technicians, NOC/SOC staff |
| **Level 4: Secure Operations** | All zones: Yellow (CP 3), Blue (CP 2), Orange (CP 4), Red (CP 5) | SCR operators, critical infrastructure engineers, data hall technicians |
| **Level 5: Unrestricted** | All zones including future/specialized areas, strict need-to-know basis | Senior security management, designated crisis management team |

### Clearance Granting Process

**Required Steps:** 1. **Sponsorship & Justification:** Formal request from authorized manager/sponsor detailing business justification and required clearance level 2. **Background Verification:** Background check commensurate with clearance level (identity verification for Level 2; extensive checks for Levels 3-5) 3. **Security Training & Acknowledgement:** Completion of mandatory security awareness training and formal acknowledgement of security policies 4. **Biometric Enrollment:** For Levels 3 and above, biometric enrollment in secure supervised environment per Section 3.6 5. **Final Authorization & Badging:** Formal authorization by Security Manager and issuance of access card/badge programmed with appropriate zone permissions

### Clearance Review & Re-certification

* All clearances reviewed annually by OT Security Lead and individual’s sponsor
* Background checks repeated periodically for high-level clearances per Security Policy

### Clearance Revocation Process

**Immediate revocation required upon:** - Termination of employment or contract - Change in role no longer requiring current access level - Violation of security policy - Request from individual’s sponsor

**Revocation initiated by HR or sponsor via formal notification to SCR. SCR immediately disables access card and biometric credentials in ACS and retrieves physical badge.**

## ACCESS CONTROL SYSTEM

### Platform

**System:** - Enterprise-grade networked system (e.g., Lenel OnGuard, Genetec, HID Global) - Redundant servers (A/B) in SCR - SQL database with backup/replication - Integration with DCIM for asset correlation

**Credentials:** - **Proximity cards:** HID or similar (13.56 MHz preferred for encryption) - **Biometric:** As specified in Section 3.6 (iris, fingerprint FAP 45+, palmprint, or facial recognition) - **Mobile credentials:** Smartphone-based access (optional for appropriate zones)

**Audit Trail:** - All access events logged (timestamp, user ID, door location, granted/denied, clearance level) - Retention: 90 days minimum (1-3 years preferred) - Exportable reports for compliance audits (SOC 2, ISO 27001, PCI DSS)

### Critical Access Points

**Main Building Entry (Man-Trap):** - **Configuration:** Double-door airlock - **Operation:** - Outer door: Card reader (Level 1-4 access) - Inner door: Card reader + PIN or biometric (Level 1-3 only) - Interlocked: Outer door must close before inner door opens (prevents tailgating) - **Fire override:** Both doors unlock on fire alarm (life safety) - **Cameras:** Coverage of both doors and interior airlock

**Data Hall Entry:** - **Security:** Card reader + PIN or biometric (two-factor authentication) - **Access:** Level 1 (facility staff) and Level 2 (customers with data hall access) - **Logging:** Entry/exit logged to DCIM (correlate with equipment changes)

**Electrical Rooms (PDMs, Transformer Rooms):** - **Security:** Card reader (Level 1 only - facility staff and authorized vendors) - **Reason:** High-voltage hazard, critical infrastructure protection

**Mechanical Rooms (Chiller Plants, Pump Rooms):** - **Security:** Card reader (Level 1 only)

**Network Operations Center (NOC):** - **Security:** Card reader + biometric (Level 1 operations staff only) - **Reason:** Command center for facility operations, security monitoring

**MPOE/MMR (Meet-Me Rooms):** - **Security:** Card reader + biometric (highest security level) - **Access:** Level 1 (facility staff), authorized carriers, escorted customers - **Reason:** Critical telecommunications infrastructure

**Storm Shelter:** - **Security:** Accessible during emergencies (fire alarm or tornado warning auto-unlocks) - **Normal access:** Card reader (Level 1-2)

### Door Hardware

**Electric Strikes or Magnetic Locks:** - Fail-safe (unlock on power loss or fire alarm) - 1,200-1,500 lb holding force (mag locks)

**Request-to-Exit (REX) Sensors:** - Motion sensors inside doors - Allow egress without card (life safety)

**Door Position Sensors:** - Monitor door status (open/closed/propped) - Alarm if door held open >30 seconds

## VIDEO SURVEILLANCE (CCTV)

### Camera Coverage

**Perimeter:** - All fence lines (360° coverage) - Gates (vehicle + pedestrian) - Building exterior walls (all sides) - Parking areas

**Exterior Critical Areas:** - Generator yard (each generator) - Chiller yard (all chillers) - 138kV substation (transformers, switchgear) - Loading dock (deliveries)

**Interior:** - All building entry/exit doors - Data hall entry doors - Data hall aisles (wide-angle, not directed into customer cages for privacy) - Electrical room entries (PDMs, transformer rooms) - Mechanical room entries - NOC interior (optional - staff monitoring) - MPOE/MMR entries - Corridors, stairwells

**Not Monitored (Privacy):** - Restrooms - Shower/locker rooms - Inside customer cages (customers may install their own cameras)

### Camera Specifications & Resolution Standards

**Standard Resolution Requirements:** - **General Areas:** Minimum 250 pixels per meter (80 pixels per foot) for identification - **Frame Rate:** Minimum 15 fps for all cameras

**Critical Point Identification Standard:**

For critical choke points where positive identification is paramount for security or audit purposes: - **Resolution:** Minimum **125 pixels per face width (PPFW)** across entire field of view where person would stand - **Frame Rate:** Minimum 20 fps (recommended to ensure clear facial capture during movement) - **Coverage Map:** Detailed Camera Coverage Map produced during design, validated during commissioning

**Critical Choke Points Requiring 125 PPFW:** - Interior of main entrance mantrap vestibule - Clean In/Clean Out (CICO) checkpoint (inspection tables and screening point) - Primary transaction window of Security Control Room (SCR) - All biometric authentication reader locations

**Fixed Cameras:** - **Resolution:** 4MP or higher (1920×1080 minimum); higher for PPFW compliance at critical points - **Type:** IP cameras with PoE (Power over Ethernet) - **Features:** - Night vision (IR LEDs, 30-50 ft range) - Wide dynamic range (WDR) for outdoor (handle bright/dark areas) - Weatherproof (IP66/IP67 rating for outdoor) - Tamper detection

**PTZ Cameras:** - **Location:** Perimeter corners, critical outdoor areas - **Features:** - Pan: 360° continuous - Tilt: -90° to +90° - Zoom: 20-30× optical zoom - Preset positions (auto-return to predefined views on alarm, perimeter breach)

### Video Management System (VMS)

**Platform:** - Enterprise VMS (e.g., Milestone XProtect, Genetec Security Center, Avigilon) - **Technology:** Option for on-prem deployment and vendor agnostic - Redundant NVR servers (A/B) in SCR - Active-active or active-passive configuration with automatic failover

**Storage:** - **Retention:** 90 days minimum (protected from unauthorized access/modification) - **Capacity:** [ROM] 100-200 TB (varies by camera count, resolution, frame rate) - **RAID:** RAID 6 or RAID 10 for redundancy - Data integrity maintained during failover events

**Features:** - Live view (single camera or multi-camera grid) - Playback with timeline scrubbing - Event search (motion detection, access control triggers) - Bookmarking (mark incidents for later review) - Export clips (for investigations, law enforcement)

**Integration:** - **Access control:** Camera pops up on access event (door opened, access denied) - **BMS alarms:** Camera view displayed on alarm (intrusion detection, equipment failure) - **SCR display:** Live camera grid on video wall in Security Control Room - **DCIM integration:** Correlation with asset access logs

### Video Analytics

**Motion Detection:** - Zones configurable (reduce false alarms) - Sensitivity adjustable

**Line Crossing Detection:** - Virtual tripwire (perimeter fence, data hall entry) - Alarm on crossing

**Loitering Detection:** - Alert if person remains in area >X minutes

**Object Left Behind:** - Detect unattended bags, packages

**Facial Recognition (Optional):** - Match faces against database (authorized personnel) - Alert on unknown person in restricted area

## INTRUSION DETECTION SYSTEM (IDS)

### Detection Devices

**Door/Window Contacts:** - Magnetic contacts on all exterior doors - Contacts on critical interior doors (electrical, mechanical rooms) - Status: Open/closed monitoring

**Motion Sensors:** - **Type:** Passive infrared (PIR) or dual-technology (PIR + microwave) - **Location:** Unoccupied areas during off-hours (offices, corridors) - **Pets immunity:** 40-80 lb (if animals on-site)

**Glass Break Detectors:** - **Type:** Acoustic sensors - **Location:** Windows (if present in offices, lobby) - **Range:** 15-25 ft per sensor

**Duress/Panic Buttons:** - **Location:** Reception desk, NOC workstations - **Function:** Silent alarm to central station + law enforcement

### Control Panel & Monitoring

**Control Panel:** - Commercial-grade (UL-listed) - Battery backup (24-hour runtime) - Cellular backup (if internet/phone lines cut)

**Central Station Monitoring:** - 24/7 UL-listed monitoring service - Alarm forwarded to central station → verifies → dispatches law enforcement - Response time: <5 minutes to central station

**NOC Integration:** - Intrusion alarms displayed on NOC workstations - NOC operator can view associated camera feeds - Manual dispatch of on-site security or law enforcement

### Alarm Zones

**Perimeter Zone:** - Fence intrusion detection, exterior doors

**Interior Zone:** - Interior doors, motion sensors (armed during off-hours)

**Critical Equipment Zone:** - Electrical rooms, mechanical rooms, MPOE/MMR (armed 24/7)

**Data Hall Zone:** - Data hall entry doors (armed 24/7 or during designated hours)

## ADVANCED FIRE AND ENVIRONMENTAL DETECTION

### Very Early Smoke Detection Apparatus (VESDA)

**Purpose:** Provide earliest possible fire warning, allowing intervention before significant damage or downtime.

**Installation Locations:** - All data halls (DH1, DH2) - All MEP rooms - UPS/switchyard areas - Red Zone critical infrastructure spaces

**System Capabilities:** - Multi-stage alerting (Alert, Action, Fire 1, Fire 2) based on predefined smoke concentration levels - Sampling pipes run above ceilings, under raised floors (if present), and within air handling units for comprehensive coverage - Integration with BMS to initiate pre-programmed responses (HVAC shutdown, door release) - Audible and visual alarms in 24/7 Network Operations Center (NOC)

**Response Protocols:** - **“Alert” level:** Visual notification, investigation by next security patrol - **“Action” or “Fire” level:** - Immediate audible/visual alarm in NOC - Activation of incident response protocols - Dispatch of on-site personnel - Zone-level location data provided to guide response

### Thermal Imaging Monitoring

**Purpose:** Proactively identify abnormal heat patterns in critical infrastructure, preventing equipment failure and fire.

**Monitoring Coverage:** - IT racks (25 kW+) - Power Distribution Units (PDUs) - Static UPS battery cabinets - Critical power infrastructure

**System Configuration:** - Fixed thermal imaging cameras providing continuous monitoring - Temperature threshold configuration with alert generation in NOC - Thermal data and alert logs retained per Security Recording Retention Policy

**Thermal Alarm Response:** - **Rack thermal alarm:** Immediate ticket to IT Operations team for affected asset investigation - **Power infrastructure thermal alarm:** - Immediate response from Infrastructure Engineers - Treated as potential P1/P2 incident (cascading failure risk) - Escalation per established incident management procedures

## SECURE NETWORK INFRASTRUCTURE FOR SECURITY SYSTEMS

The electronic security systems are critical infrastructure requiring protection from cyber threats that could compromise physical security.

### Physically Separate and Logically Segmented Network

**Network Separation:** - All electronic security systems (ACS, CCTV, IDS, management servers) operate on network physically separate from: - Corporate IT networks - Operational technology (OT) networks - Guest networks - Logical segmentation (VLANs with strict firewall rules) where physical separation not fully feasible - Design goal: maximum isolation

**Network Inaccessibility:** - Security systems network inaccessible from internet and any non-security internal networks - Data exchange (monitoring dashboards, log aggregation) facilitated through: - Tightly controlled unidirectional or bidirectional data diode, OR - Demilitarized zone (DMZ) with robust firewall policies - No direct network routing between security and other networks

**Protected Network Infrastructure:** - Core network infrastructure (switches, routers, firewalls) for security systems: - Located within access-controlled Red Zones - All unnecessary ports and services disabled - Hardened configurations per industry best practices

**Power Resilience:** - Entire security systems network infrastructure (all active network components and endpoint devices) powered by: - Facility UPS systems - Backup generators - Ensures continuous operation during mains power failure

**Security Monitoring:** - Security systems network monitored for: - Unauthorized access attempts - Anomalous traffic patterns - Logs from network security devices (firewalls) aggregated and reviewed - Integration with Security Operations Center (SOC) monitoring

## PHYSICAL PROTECTION OF SECURITY SYSTEM COMPONENTS

All field devices and interconnecting infrastructure must be physically protected against tampering, sabotage, and environmental damage.

### Tamper-Proof Enclosures

**Requirements:** - All field devices installed in tamper-proof enclosures: - Access control readers - Intercoms - CCTV cameras - Intrusion Detection System (IDS) panels - Motion detectors - Enclosure construction: hardened steel or polycarbonate materials - Integrated tamper switches on all enclosures - Unauthorized opening, removal, or impact generates immediate tamper alarm in SCR identifying specific device

### Protected Cabling and Conduit

**Cabling Protection Requirements:**

**Mandatory Rigid Steel Conduit Locations:** - All exterior areas - Vulnerable locations (loading docks, publicly accessible lobbies, perimeter fences) - Pathways above accessible ceilings - Entire Violet Zone (CP 1)

**Interior Access-Controlled Zones (Yellow, Orange, Red):** - Minimum: Armored cable (SWA) or conduit - Continuous conduit runs, securely grounded

**Network Infrastructure Access:** - Network infrastructure (switches, patch panels) supporting security system: - Housed within locked cabinets - Located in access-controlled Red Zones - Access restricted to authorized personnel only

### Secured Mounting and Accessibility

* Devices mounted at height/orientation minimizing physical damage risk while maintaining operational effectiveness
* Critical components elevated or recessed where possible
* Service access controlled and logged

## SECURITY PERSONNEL & GUARD POSTS

Security personnel are integral to physical security system effectiveness. Fixed guard posts established at strategic locations for continuous monitoring, intervention, and procedural enforcement.

### Primary Guard Posts (Mandatory)

**Main Gatehouse (Violet Zone):** - **Location:** Main vehicle entrance sally port - **Configuration:** Climate-controlled, hardened guard post - **Equipment:** - Duress alarms - Communications equipment - Direct control of vehicle sally port and pedestrian gates - Government ID verification capability - **Responsibility:** Initial vehicle and personnel verification

**Security Control Room (SCR) (Red Zone):** - **Function:** Primary central monitoring station (see Section 8.2) - **Responsibility:** - Overall system monitoring - Alarm response - Dispatch of roving patrols - 24/7 continuous operation

**Clean In/Clean Out (CICO) Checkpoint (Orange Zone):** - **Function:** Dedicated security position within CICO checkpoint - **Responsibility:** Equipment and personnel screening per Section 6.2 - **Staffing:** Manned during all data hall operational hours

### Secondary/Roving Patrols

**Patrol Coverage:** - Violet Zone (perimeter, generator yard, parking lots) - Red Zone (loading dock, mechanical spaces) - Other critical areas per site security plan

**Patrol Requirements:** - Routes, schedules, and check-in points defined in Security Operations Manual - Check-ins using fixed or handheld readers for accountability - Integration with SCR dispatch system

## SYSTEM MAINTENANCE, LOGGING & PERFORMANCE MONITORING

### Scheduled Maintenance

**All electronic security systems (ACS, CCTV, IDS) maintained per:** - Manufacturer specifications - Vendor support agreements

**Preventive Maintenance Schedule:** - **Quarterly:** System health checks and performance validation - **Bi-annual:** Hardware inspection and cleaning - **Annual:** Comprehensive system testing and calibration

### Maintenance Logging

**All maintenance activities formally logged:** - Date, time, and duration - Personnel involved and work performed - System components affected and changes made - Pre- and post-maintenance system status - **Retention:** Minimum 3 years (audit support)

### Failure Response

**Procedures for system failures:** - Immediate notification to SCR - Implementation of temporary security measures within 2 hours - Full system restoration within 24 hours for critical systems - Documentation of failures and compensatory controls for audit

### Performance Monitoring

**System performance continuously monitored against established KPIs:** - System availability and uptime statistics - Response time metrics for access control systems - Video surveillance system recording integrity - Intrusion detection system false positive rates - **Reporting:** Quarterly performance reports per Security Policy

## CUSTOMER CAGE SECURITY

### Physical Separation

**Cages:** - **Material:** 8-10 ft high steel mesh partitions (wire mesh or expanded metal) - **Mesh size:** <2” × 2” (prevents hand/tool reach-through) - **Roof:** Ceiling-mounted mesh or solid lid (prevents climbing over) - **Floor:** Slab-on-grade (no raised floor under cages, prevents tunneling)

**Doors:** - Lockable cage doors with card readers - Customers manage their own user credentials - Audit trail: Access events logged and available to customer via DCIM portal

**Size:** - Variable (4-cabinet, 8-cabinet, 12-cabinet cages) - Custom layouts per customer requirements

### Access Control

**Customer-Managed:** - Customers assign/remove user credentials for their cage - Facility provides card reader hardware and database integration

**Facility Escort (Optional):** - Customer visitors must be escorted by customer staff or facility staff

### Surveillance

**Data Hall Cameras:** - Provide general aisle coverage (not directed into cages for privacy) - Customer may install internal cameras if desired

## INTEGRATION WITH BMS/DCIM/FIRE ALARM

### Centralized Monitoring (NOC)

**Single-Pane-of-Glass:** - All security systems accessible from NOC workstations - Video wall displays: - Live CCTV grid - Access control alarm panel - Intrusion detection status - BMS/DCIM alarms

**Alarm Correlation:** - Access event → Camera pops up - Intrusion alarm → Camera preset to zone - Door forced open → Camera + alert to NOC

### Automated Responses

**Fire Alarm Override:** - All access control doors unlock on fire alarm - Security system prioritizes life safety egress

**Intrusion Alarm + Camera:** - Intrusion sensor triggered → Camera switches to live view on NOC screen

**After-Hours Mode:** - Interior motion sensors armed automatically (scheduled) - NOC notified of any motion detection

### Audit & Compliance

**Logging:** - All access events, video footage, intrusion alarms logged - Exportable reports for SOC 2, ISO 27001, PCI DSS audits

**Retention:** - Access logs: 1-3 years - Video: 90-180 days - Intrusion events: 1-3 years

## COST SUMMARY (HIGH RISK SITE)

|| System | Cost Estimate | Notes | ||——–|—————|——-| || **Perimeter Fencing (8 ft + Anti-Climb + Anti-Dig Barrier)** | $300-500K | HR requirement: 100 ft standoff, anti-dig barrier | || **Perimeter Berm (HR Requirement)** | $150-250K | Earthen berm, integrated with grading | || **Sally Port (Dual-Gate with K4 Arrestor)** | $200-350K | HR requirement: interlocking gates | || **Permanent Visitor Center (Gatehouse)** | $150-250K | HR requirement: climate-controlled, hardened | || **Full-Height Turnstiles (Pedestrian Gates)** | $50-100K | HR requirement | || **Line-of-Sight Intrusion Detection** | $100-200K | Perimeter-wide coverage | || **Vehicle Barriers (K4/K12 Bollards)** | $150-250K | Critical infrastructure protection | || **Access Control System (Redundant, Biometric)** | $300-500K | Redundant servers, MFA, clearance levels 1-5 | || **Video Surveillance (100-150 Cameras, Redundant NVR)** | $500-800K | 125 PPFW critical points, thermal cameras, redundant storage | || **Security Control Room (SCR) Infrastructure** | $200-350K | Redundant systems, 99.982% availability, hardened construction | || **CICO Checkpoint Equipment** | $75-150K | Magnetometer, screening equipment, UPS-backed | || **Intrusion Detection System (Enhanced)** | $100-200K | Secondary sensors, tamper-proof enclosures | || **VESDA Systems** | $150-250K | Data halls, MEP rooms, UPS areas | || **Thermal Imaging Monitoring** | $100-200K | Racks 25kW+, PDUs, battery cabinets | || **Secure Network Infrastructure** | $100-150K | Physically separate, redundant switches, firewalls | || **Customer Cage Infrastructure** | $100-200K | Mesh partitions, access control | || **Integration with BMS/DCIM/Fire** | $75-150K | Unified monitoring platform | || **Guard Posts (Furniture, Equipment)** | $50-100K | Main gatehouse, SCR, CICO positions | || **Physical Protection (Conduit, Tamper Enclosures)** | $100-150K | Rigid steel conduit, tamper-proof housings | || **Central Station Monitoring (Annual OPEX)** | $10-20K/year | 24/7 UL-listed service | || **Security Personnel (Annual OPEX)** | $500K-1M/year | 24/7 coverage (3 posts + roving patrols) | || **Total Security Systems (CAPEX)** | **$2.9M-4.8M** | High Risk site with Tier III availability |

**Notes:** - Costs reflect High Risk (HR) site requirements per Security Narrative - Enhanced perimeter security (berm, sally port, permanent gatehouse) adds ~$500-850K vs. Medium Risk - Redundant systems for 99.982% availability adds ~$300-500K - VESDA and thermal monitoring adds ~$250-450K - Biometric MFA and clearance-level ACS adds ~$150-200K vs. card-only - Security personnel OPEX is ongoing operational cost (not included in CAPEX total)

## CODES AND STANDARDS

* **UL 294** (Access Control System Units)
* **UL 2050** (Intrusion Detection Equipment)
* **NFPA 730/731** (Security System Installation and Monitoring)
* **ASTM F2656** (Vehicle Barrier Crash Testing)
* **TIA-942** (Data Center Security Requirements)
* **SOC 2 Type II** (Physical Security Controls)
* **ISO 27001** (Information Security Management - Physical Security)
* **PCI DSS** (Payment Card Industry - Physical Security Requirements)

**Tags:** #pryor-dc #security #access-control #cctv #intrusion-detection #perimeter-security

**Next Steps:** 1. Select access control and VMS platforms (single vendor preferred for integration) 2. Design camera layout with coverage analysis (blind spot identification) 3. Coordinate crash-rated bollard locations with site civil design 4. Develop access control policy (credential issuance, escalation procedures) 5. Obtain quotes from UL-listed central station monitoring services

**Document Control:** - **Source:** Pryor\_Bod\_EVS\_Rev01.md and Erik\_BOD reference - **Date Updated:** October 29, 2025 - **Prepared by:** EVS / PGCIS Team - **Key Updates:** Man-trap design, customer cage security, SOC 2/ISO 27001 compliance