


SECURITY SYSTEM DESIGN GUIDELINES

Washington State Department of Corrections

State Project Number 2011-320A

VERSION 1.0 - June 30, 2011

design groups, inc. p.s.
architecture
education facilities group
justice facilities group
security design group
828-7th Avenue SE
Olympia, WA 98501
360.352.8883

TABLE OF CONTENTS

Washington Department of Corrections
Security System Design Guidelines

TABLE OF CONTENTS

i. Summary and Overview

These Design Guidelines were developed by the Washington Department of Corrections (WSDOC) for use in its projects of any scope or scale, which involve or affect Security Systems. They are intended to create consistency in the design and application of Security Systems across the full range of DOC's correctional facilities, encompassing Community Corrections, Work Camps, standalone Institutions, and multi-custody level Correctional Complexes.

KMB design groups, inc., p.s., with the specialized expertise of its subconsultants, organized worksessions attended by stakeholders representing a broad base of knowledge and interest, who collectively, and with great diligence, developed and refined this document.

The Guidelines convey the Agency's goals, expectations, and requirements regarding both the design and the implementation of systems that are critical to its ability to achieve its mission and objectives.

The Guidelines are not prescriptive requirements, but rather are documentation of the collective current consensus as to what WSDOC believes will best meet its needs and provide an appropriate pathway to the future, with regard to Security Systems. Deviations from the Guidelines may be appropriate in some circumstances, so a process for Owner review and consideration of alternatives and exceptions is provided.

This document is not static…..the evolution of technology, and the constant striving for improved ways of doing business and increasing safety and security, will need to be reflected through periodic updates. Feedback from users of the Design Guidelines is encouraged, to make this an even better document.

ii. Acknowledgements

These Design Guidelines are the outcome of a true collaborative effort on the part of many individuals, with the full support of their chain-of-command. We are grateful for the significant contributions to this document by:

Washington State Department of Corrections

Kent Nugen, Chief of Capital Programs / GA DAD

Ed Hampton, Project Manager, Capital Programs

Wayne Pederson, RCDD, Capital Programs

Peter Jekel, DOC IT Security

Rick Smith, DOC IT Security

Lorraine Louderback, DOC WAN Team

Amy Bosler, DOC Network Group

Capt. Mike Green, Washington Corrections Center for Women, Custody

Kevin Loresch, Monroe Correctional Complex, Plant

Dan Doll, Washington State Penitentiary, ET

Karl Lofgren, Stafford Creek Corrections Center, ET

Cal Archer, Airway Heights Corrections Center, ET

Consultant Team

Bob Welt, PE, MW Engineers, Principal

Dan Beamer, MW Engineers

Steve Helms, PE, DEI Electrical Consultants, Principal

Patrick Shannon, RCDD, PMP®, MCSE, Hargis Engineers, Sr. Associate - Telecommunications

Jason Ramay, AIA, KMB design groups, Associate

Steve Anderson, AIA, CSI, KMB design groups, Principal, Design Guidelines Project Director

iii. Definitions and Abbreviations

802.11	Standards for a Wireless Local Area Network (WLAN)
ACA	American Correctional Association
Agency	State of Washington Department of Corrections, when used herein
API	Application Programming Interface
Appliance	A computing device with a specific function and limited configuration ability
Aspect Ratio	The ratio of width of an image to its height (ex: 4:3, 16:9, etc)
Bandwidth	A bit rate measure of available or consumed data communication resources
BEP	Building Entrance Protection
BICSI	Formerly Building Industry Consulting Service International, Inc., now an international association serving the IT industry through education, certification, and technical publications
Bit	Bit (and Megabit) are measures of units of information typically related to transport capacity and associated with a time element (i.e. 100 megabits per second). There are 8 bits in a byte.
Blu-Ray	An optical disc storage media
Byte/KB/MB/TB/GB/PB etc.	Byte(s), Kilobytes, Megabytes, Terabytes, Gigabytes, and Petabytes are measures of units of information, typically related to digital storage or capacity (i.e. a 250GB hard drive). A single byte contains 8 bits.
CATV	Cable (entertainment) television
CCxx	Certifications for Cisco IT Professionals, where xx = the specific certification attained
CCTV	Closed Circuit Television – also Security Video System
Change Control	Formal process used to ensure that changes to a product or system are introduced in a controlled and coordinated manner.
CIF	Common Intermediate Format (video image size)
Client	(as in Client-Server) a machine which operates in conjunction with a server
Codec	A device or computer program capable of encoding and/or decoding a digital data stream or signal
Cold Spare	A spare which is fully prepared but is not stored in a powered-up state
Contractor	See Security System Contractor
Control Point	In this document, any location that has an interface to the Security System for supervisory monitoring or operational control
COTS	Commercially available Off-the-Shelf (as in hardware or software that is a standard product sold in substantial quantities in the commercial marketplace and therefore readily procured through open purchasing channels)
Design Team	In this document, the entire design consultant team inclusive of the Architect or Engineer who is the prime consultant, operating under an agreement for professional services with the State of Washington, for the benefit of the Department of Corrections
Designer	See Security System Designer
DOC	Department of Corrections (reference is to State of Washington Department of Corrections when used herein)
DPS	Door position switch

DVD	Digital Video Disc, an optical data storage media
DVR	Digital Video Recorder, a device capable of viewing and digitally recording analog video channels
Enterprise	A unit of economic organization; especially: a complete business organization
ET	Electronics Technician
EMI	Electromagnetic Interference
Ethernet	Wiring and signaling standards for the Physical Layer of the standard networking model
FA	Fire Alarm
FACP	Fire Alarm Control Panel
FAR	False Alarm Rate
Firewall	Devices or software designed to permit or deny network transmissions based upon a set of rules, frequently used to protect networks from unauthorized access while permitting legitimate communications to pass
Firmware	Low-level device operations software
GUI	Graphical User Interface
HA	High Availability
H.264	A standard for video data compression
HMI	Human-Machine Interface
Hot Spare / Hot Standby	A hot spare or hot standby is used as a failover mechanism to provide reliability in system configurations; the hot spare component is active and connected as part of a working system
Hot Swapping	The function of replacing computer system components without shutting down the system
HQ or HQ/IT	In this document reference is to the Washington Department of Corrections Headquarters' designated staff; HQ/IT refers to designated Information Technology staff normally based at DOC Headquarters
HVAC	Heating, ventilation, and air conditioning
HVR	Hybrid Video Recorder – similar to a DVR, but capable of incorporating digital IP cameras in addition to analog video inputs, for viewing and recording operations
IDF	Intermediate Distribution Frame
Integrator	See Security System Contractor
IP	Internet Protocol
ISB	Information Services Board (WA)
ISDN	Integrated Services Digital Network (ISDN) is a set of communications standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network.
ISS	Integrated Security System – see also Security System, below
iSCSI	Internet Small Computer System Interface, an Internet Protocol (IP)-based storage networking standard for linking data storage facilities
IT	Information Technology (see also HQ/IT and Local IT)
ITRP	Information Technology Replacement Program

JPAY	An Inmate Services kiosk system
KVA	Kilo-volt amp
KVM	Keyboard-Video-Mouse, as in a KVM extender to remote the human interface devices at a location away from the CPU
LAN	Local Area Network
Layer 3	The Network Layer of the seven-layer OSI model of computer networking
Local IT	In this document refers to DOC's Information Technology staff normally assigned to the facility or region where the project work is to occur (see also HQ/IT)
MACC	Maximum Allowable Cost (part of the capital project budget)
Malware	Malicious software
MCR	Master Control Room or Main Control Room
MDF	Main Distribution Frame
Mirrored	Duplicative
Mobile Map	A portable device with status indication and alarm annunciation on a map graphic
NAR	Nuisance Alarm Rate
NC	Normally closed (contact)
NO	Normally open (contact)
NTP	Network Time Protocol
NVMS	Network Video Management System (also VMS)
NVR	Network Video Recorder
OC gas	Non-lethal "pepper spray" agent
OFCI	Owner furnished, contractor installed
OFOI	Owner furnished, owner installed
ONVIF	Open Network Video Interface Forum
Open distribution channel	Where the product's distribution is not restricted to a limited number of entities
OS	Operating system
Owner	Where used in this document refers to a designated representative of the Washington Department of Corrections
P2V	Physical-to-virtual (migration of a physical server's OS, applications, and data from a physical server to a virtual machine guest hosted on a virtualized platform)
Patch	A piece of software designed to fix problems with, or update a computer
Patch management	Managing the deployment (which may be automated) of Patches
PC	Personal Computer
PIDS	Perimeter Intrusion Detection System
PDA	Portable Digital Assistant
Peer-to-Peer	Interconnected devices where neither functions as a Server
PIO	Public Information Officer
PIR	Passive Infrared
PLC	Programmable Logic Controller, a digital computer used for automation of industrial processes
POD	Probability of Detection

PoE	Power over Ethernet
PREA	Prison Rape Elimination Act
PROX	Proximity
PTZ	Pan-tilt-zoom
RAID-xx	Redundant array of inexpensive disks, where xx is the Level
RCDD	Registered Communication Distribution Designer
REX	Request to Exit (a device providing input to a security control system)
RF	Radio Frequency
RFC	Request for Change, one of the processes or documents in Change Control within IT service management
RFID	Radio Frequency Identification
Router	A network device managing the delivery of digital packets
RS-232	A serial communications standard
RS-485	A digital communications network standard
SAN	Storage Area Network
SAW	Surface Acoustic Wave
SCADA	Supervisory Control and Data Acquisition
Security System	Collectively, all of the components, software and programming that comprise electronics for the purposes of detection, monitoring, surveillance, controlling, and communicating for prison operational security (may also be referred to as an Integrated Security System)
Security System Designer	The qualified design professional(s) whose responsibility is design of the Security System; may be a sub-consultant to an architect or engineer who is the prime consultant contracted to WSDOC
Security System Contractor	The Contractor (who may be a subcontractor to the General Contractor and who may employ other entities as sub-subcontractors for portions of the Security System work) who is the responsible entity for the integration and construction installation, testing, and delivery of the Security System for the project
Security Video System	The system providing live imaging for security purposes, and which may also archive (record) video images for playback
SensorCoil®	A proprietary coiled stainless steel razor ribbon with embedded sensor
Server	A computer in a network that is used to provide services to other computers in the network
SLA	Service Level Agreement
SPD	Surge protection device
SQL	Structured Query Language, a database computer language
SSL	Secure Socket Layer
Stress Test	To prove in a high-demand test simulation
Surge	Short duration voltage spike
TWIDS	Taut Wire Intrusion Detection System
TCGS	Telecommunications Construction Guide Specifications
TDDG	Telecommunications Distribution Design Guide
TDIS	Telecommunications Distribution Infrastructure Standards
TGB	Telecommunications Grounding Busbar
TGMB	Telecommunications Main Grounding Busbar

TIA	Telecommunications Industry Association
UG	Underground
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
UTC	Coordinated Universal Time
Virtualization	The creation of a virtual (rather than actual) version of something
V-LAN	Virtual Local Area Network
VMS	Video Management Software (also NVMS)
VPN	Virtual Private Network
WA	State of Washington
WAN	Wide Area Network
WSDOC	State of Washington Department of Corrections
"Zero Client" Workstation	A Thin Client "Zero Client" machine which accesses a remote Desktop which is virtualized on a (remote) server

Note: Throughout the Guidelines reference is made to product names, manufacturers, and organization names which are trademarked by their respective owners. Such reference is in no way intended to usurp any rights accruing to the trademark holder.

I. Intent and Application

A. Statement of Intent

These Security System Design Guidelines are to be provided by the Washington Department of Corrections' Capital Project Manager to the prime consultant at the inception of a project which will include design of Security Systems. There should be further distribution to any project design team members who will be involved with Security System design, the environments in which they will be deployed, and the infrastructure, devices, and facility components with which they are integrated.

Much of the language of the Guidelines is directed to the Security System Designer, but with recognition that that entity may in-fact be a sub-consultant under the prime consultant who is contracted to WSDOC. The Guidelines do not intend to usurp any agreements, or establish any flow of project information that precludes good communication and coordination between the design team parties. Such language should be construed that the prime consultant is expected to understand and follow the Guidelines, with the Guidelines anticipating that the Security System Designer is the member of the design team best suited to carry out the Guidelines as set forth.

The intent of the Guidelines is to establish a foundation for the design team, and particularly the Security System Designer, to understand WSDOC's expectations, goals, and the constraints, relative to designing Security Systems in correctional facilities for the State of Washington, regarding,

- the systems to be designed (both from an operational basis and a technical requirements basis),
- the design process, and
- aspects of the construction implementation that are deemed by the Agency to be critical to achieving a successful project involving Security Systems.

It is very important to WSDOC, for a number of reasons, to have Security Systems in its facilities that are consistent, including the technical configuration and components, the quality and performance, and how the operator/user interfaces with the Systems. However, it is recognized that each facility has a unique mission and, in the case of existing facilities, a unique circumstance of infrastructure and existing/legacy systems and components, which may lead to special design considerations and solutions. Each project will also have a different scale and scope. These Guidelines provide for those circumstances.

> *It is NOT intended that these Guidelines be used as a prescriptive method of design. Also, they are NOT specifications, and they should NOT be referenced by the project specifications. They are Guidelines to assist the DOC project manager, the DOC facility staff, other Agency stakeholders, and the design team, throughout the project design phases, and to provide guidance for the Owner's expectations during project construction implementation.*

It is the responsibility of the design team to determine the applicable safety and health practices and the life-safety considerations associated with design of Security Systems, and to adhere to applicable regulatory requirements.

WSDOC recognizes the benefits of thoughtful design and engineering provided by its consultant teams, and believes that the best project outcome will come from full utilization of the skills and experience of the design team to meet the project goals and requirements, with these Guidelines providing a framework and process.

B. Current "State-of-the-Art" and Moving Toward the Future

Security Systems in correctional facilities are expected to extend, through electronic monitoring and automation, the capabilities of staff far beyond what can otherwise be accomplished using traditional "boots-on-the-ground" and key-operation methods. With proper design they can provide a very high degree of

operational support and flexibility. The Security System is critical to safety and security for staff, the offenders, and the public.

Correctional facilities being operated in Washington include institutions constructed between 1885 and the present. All have been expanded or modified since their original construction. For many of the older facilities, the changes may have occurred multiple times for any given building or portion of the site. Often there has been a re-purposing of a facility component, or a change in the security level for its operation. This, as well as changes in design approach and available technology over time, causes a wide variety of conditions to exist in the State's facilities.

Recent major projects have set the "state-of-the-art" for Security Systems in Washington's correctional facilities to be:

- A taut-wire perimeter detection system incorporating microwave detection at gates (for Level-3 and above facilities)
- A fully networked PLC/touchscreen control and monitoring system with all Control Points inter-linked
- A digital, networked, intercommunication system
- A fully digital IP video system with IP cameras and network viewing and recording
- Proximity card automated access control system for Staff access control at selected areas
- Database integration at some Level-4 and all Level-5 housing units

Many existing DOC facilities have standalone control and monitoring points which have control panels and electronic systems based on switches and relays for control logic. The control system may have limited or no integration of video switching, and the video is often local-only and of low resolution analog (in some cases black-and-white) with limited or no recording capability. Older intercommunication systems are often built-up from proprietary components, with relay switching.

It is the Agency's intent to move older Security Systems toward the "state-of-the-art" to the greatest degree feasible given the project scope, funding, and legislative intent. The design team should be very conscious in setting project priorities that security and safety is the highest priority, with operational flexibility and life-cycle cost also very high in priority.

Further, it is the intent of the Agency to make provisions for the continuing evolution of technology, and for the beneficial expansion of system capabilities that will become available or viable in the future that will better support its mission in public safety.

C. Application to Different Project Scales and Scopes

The Department of Corrections maintains a 10-year Capital Plan which is updated every two years. Non-emergency capital projects are proposed by the Department for funding in the biennial budget based on prioritized overall Agency programmatic needs, or to address facility needs that are preservation in nature. The project scope statement and any Legislative Notes accompanying the appropriation becomes the guideline for what must be accomplished by the project. Expansion of the scope beyond that which is reasonably inferred by the scope statement, even if it can be accomplished within the available funding, requires the Agency to seek prior approval.

1. <u>For New Institutions or Major Expansions of Existing Institutions – Original Design</u>

   Follow these Guidelines.

2. For Projects Within Existing Facilities – New Design or Retrofit/Upgrade of Existing

   An initial "scope verification" step should occur as soon as practical after the design services agreement is authorized. The Security System Designer (and the prime consultant) should undertake a thorough review and assessment of Owner data, and make onsite verification visits as necessary to ascertain the existing Security System configuration(s) and conditions, and the existing, or opportunities available for, connectivity and integration with other onsite Security Systems or components. The Security System Designer should combine the initial project scope statement with the results of the assessment, make a comparison with these Guidelines, and develop an outline "Security Systems Scope of Design" for review with the DOC project manager.

   For these projects the expectations of the Agency are that:

   - Equipment rooms for Security System components should conform to these Guidelines
   - Relay-logic control and monitoring should be replaced with networked or network-capable Programmable-Logic-Controllers (PLC's)
   - "Built-up" circuit-board intercommunication switching should be replaced with digital switching
   - Video cameras, whenever feasible, should be digital IP type; existing analog cameras converted to digital IP by encoding hardware will be considered
   - Video viewing should be digital, from the network
   - Video transmission between buildings should be digital, on an Ethernet network
   - Video recording should be to a centrally managed digital Network Video Recording system (not including Digital Video Recorders) with storage capacity accommodating all video originated by this project (and any existing cameras retained) at the frame rate and resolution described in these Guidelines. The storage capacity should provide the archive retention time described in these Guidelines (if network connectivity to an existing central system is not viable, or a central system is not existent, consider creating a local node which can be incorporated into a facility-wide system in the future)
   - The control and monitoring, intercommunication, and video components that are digital should operate on standard Ethernet network infrastructure compliant with DOC's TDIS requirements
   - Operator interface(s) should be determined based on system complexity, functionality, flexibility, facility operations, and for potential future modifications, as well as cost
   - All portions of the Security System, including devices controlled or monitored by the System (inclusive of locking systems), should be supported for power requirements by an Uninterruptible Power Supply (UPS)
   - The quality and reliability standards expressed in these Guidelines should not be compromised.

II. Agency Goals and Requirements

A. Agency Goals

To fulfill their mission and responsibilities at the lowest total cost of operation WSDOC seeks to achieve the following in connection with its projects involving Security Systems:

- Reduce dependency on Contractors for non-warranty maintenance, repairs, and system adds/changes
- Utilize standardized Enterprise level Systems
- Utilize, to the greatest extent possible, Systems which operate on COTS hardware and utilize as their basis COTS software, which can be sustained by the Agency
- Receive Security Systems that are expandable and adaptable to changing needs
- Receive Systems which are configured with common platforms, interfaces, and physical and logical configurations within a facility, and move toward commonality Agency-wide
- Leverage the Agency's investment in IT infrastructure by sharing physical and human resources for support of Security Systems
- Leverage the information contained within Agency databases in ways that support more efficient and effective security operations.

B. Related State or Agency-Adopted Policies and Standards

1. Prior to engaging in any design activities related to the WSDOC, the design team should familiarize themselves with the relevant DOC policies that are in place. At a minimum, the Security System Designer should become familiar with the following DOC Policies, which can be readily accessed via the DOC website, http://www.doc.wa.gov. (Note: These policies are updated and replaced frequently; the Security System Designer shall be responsible for reviewing the current policies in place at the time of design.)

   - 280.100 – Acceptable use of technology
   - 280.250 – Acquisition, Disposal, and Licensing of Information Technology
   - 280.300 – Information Technology Disaster Recovery
   - 280.310 – Information Technology Security
   - 280.825 – Technology Governance
   - 280.925 – Offender Access to Electronic Data
   - 400.030 – Security Guidelines for Wireless Portable Technology in Facilities
   - 420.450 – Audio Monitoring
   - 700.130 – Electrical Construction and Maintenance

2. In addition to the policies noted above, WSDOC has developed internal standards related to network connectivity, pathways, space requirements, and wiring to support electronic systems. These standards are titled "Washington State DOC Telecommunications Distribution Infrastructure Standards" and are commonly referred to as the TDIS.

3. The methodology and approach documented in the TDIS is a requirement for all network based connectivity installed at DOC facilities. This document is quite specific and contains requirements beyond those addressed by the ANSI/TIA/EIA standards bodies, and national codes such as the NEC and NESC.

4. The TDIS includes very specific training and credentialing requirements for designers, including requirements for specific elements of the designs to be performed by a qualified Registered Communications Distribution Designer (RCDD). Project design teams not already familiar with WSDOC's requirements should review the specific requirements included in the TDIS, as it may shape the manner in which the design efforts are accomplished.

5. Being a state agency, the DOC is also required to follow the policies and standards of the Washington State Information Services Board (ISB), as it relates to information technology infrastructure. The ISB was created by the state Legislature in 1987 and given the authority for policy development, strategic IT planning, oversight of the executive branch agencies' IT projects, and for delegating authority to agencies for IT investments. The Security System Designer is expected to provide system design and anticipated cost information to the regional IT/Infrastructure specialist to support the internal relationship between the ISB and the DOC.

6. Designers shall work with the DOC stakeholders to ensure these requirements are met. At a minimum, the Security System Designer should become familiar with the following ISB requirements, which can be found at http://www.isb.wa.gov. (Note: These requirements are updated and replaced frequently; the Security System Designer shall be responsible for reviewing the current policies in place at the time of design.)

    - 400-P1 – IT Security Policy
    - 401-S1 – IT Security Standards
    - 402-G1 – IT Security Guidelines
    - 500-P1 – IT Disaster Recovery and Business Resumption Planning Policy
    - 501-S1 – IT Disaster Recovery and Business Resumption Standards
    - 502-G1 – IT Disaster Recovery and Business Resumption Guidelines
    - 700-P1 – Computing and Telecommunications Architecture Policy
    - 701-S1 – Computing and Telecommunications Architecture Standards – Building Wiring
    - 702-S1 – Computing and Telecommunications Architecture Standards Database Management
    - 704-S1 – IT Standards and Protocol Directions
    - 1003.2-S – Integration Architecture Standards
    - 1104.0-S – Network Standards

7. The requirements of WSDOC and the State of Washington may differ from other current nationally recognized "generic" standards utilized in private enterprise. As such, the documents noted above contain vital information that may not be known to designers that are not familiar with these State of Washington agencies.

8. These Guidelines and requirements do not relieve or in any way alter the responsibility for the design and construction to comply with all applicable state and/or federal standards and regulations.

III. Design Phase Collaboration, Reviews, and Alternative Design Proposals

A. Collaboration for Owner Furnished Services and Equipment

1. Stakeholders

- DOC HQ Enterprise Network Communication (ENC)
- DOC HQ Infrastructure Specialist
- DOC HQ IT Procurement
- DOC Project Manager
- Facility Plant Manager
- Facility IT Support
- Facility Security Electronics Support
- Security System Designer
- Structured Cabling Designer (RCDD)

2. Services and Roles

Security System Designer shall organize and lead meetings as necessary, and at appropriate times during the project design phases, to determine responsible parties for different aspects of network design (DOC or A/E team), to track and update progress, and to facilitate open communications among the stakeholders for:

- WAN Connections and Infrastructure
- LAN Connections and equipment
- IP Addressing
- V-LAN Strategy
- VPN Strategy
- Network Security/Credentialing
- Other Network Integration
- Procurement method for equipment and hardware
  - Routers
  - Firewall
  - Switches
  - PC Workstations
  - Servers
  - Cabling and Patchcords

The Security System Designer shall, as part of his services, determine range-of-magnitude level costs for owner-provided equipment, and coordinate with the DOC Project Manager for setting an appropriate allocation of the project's funding for the equipment.

B. Required Systems Design Presentations / Reviews

1. The required Systems Design Presentations and Reviews for Security Systems shall, unless otherwise specified by the DOC project manager, follow the same schedule as regular design phase reviews and approvals. Typically, these reviews take place at the conclusion of the pre-schematic scope refinement,

schematic design, and design development phases, and at multiple points during the construction documents phase, with additional partial phase reviews as decided by the Project Team or indicated by the size and scope of the project.

2. The Security System design presentations and reviews should be dedicated exclusively to the Security Systems and their relationships to other project systems and design elements.
3. In addition to the Security System Designer and the DOC project manager, the presentations and reviews should include, at a minimum, other key participants from DOC, including: IT Infrastructure Specialist, Facility Manager, Facility Information Technology (IT), Facility Electronic Technician (ET), Facility Administration, and Facility Custody.

C. QA / QC and Peer Review of Design

1. The project design team, including the Security System Designer, shall conduct a transparent and published QA/QC in-house review of the project design prior to the delivery of the phase submittals. The products of this review process shall be available to the DOC project manager by request. In addition, the DOC may request a Peer Review of the documents near project completion. (Larger capital projects require a "Constructability Review".)
2. In the case of Peer Review of the design, the DOC shall deliver to the project design team leader the review document and afford the design team time to respond to any suggested changes in the design.

D. Alternatives and Exceptions to the Guidelines, Procedures

1. The DOC does not adhere to a particular set of design standards for security systems or other facility systems, e.g., American Correctional Association (ACA) standards. The Security System Design Guidelines are not a prescriptive document, nor do they specify the applications to be included in individual projects. DOC understands that the expertise of the design team will produce valuable, project-specific ideas, and wishes not to preclude alternatives and exceptions to the requirements listed here. Rather, the guidelines encourage the design team to seek optimal solutions, to be reviewed and assessed as follows.
2. For all proposed alternatives and exceptions to these Guidelines, the Security System Designer should make the DOC Project Manager aware of the issue as early as possible in the design schedule in order to allow adequate time for a complete presentation, analysis, and decision. The process for securing an approved alternative or exceptions to these Guidelines shall be as follows:
    a. Security System Designer proposes, in detail the alternative or exception, referencing to the Guideline(s) with which it varies.
    b. The DOC project manager may accept or reject the proposed alternative or exception OR convene a decision group composed of project stakeholders, DOC personnel, and/or independent consultant(s).
    c. If convened, the decision group accepts, with or without conditions, or rejects the proposed alternative or exception.
    d. Proposed alternatives or exceptions to these Guidelines should follow a detailed review process that includes, at a minimum:
        - Evaluation of the proposed products or systems to ensure that the proposed systems are not either obsolete or unproven.
        - Performance rationale for the proposed variance.

- Cost analysis of the proposed variance.
- The effect(s), if any, on other project systems or Guidelines.

e. The Security System Designer records the result of the decision process and documents any approved alternatives and exceptions.

f. DOC reviews the alternative or exception for inclusion in, or modifications to, later editions of these Guidelines.

IV. Design Criteria

A. Open Architecture

Fundamental to a sustainable long-term integrated electronic security solution, Security System Designers should make every effort to specify systems, transport, devices, and an architecture, that is non-proprietary in nature. Software and hardware infrastructures that demonstrate an open architecture and wide interoperability, as well as generally unrestricted support verticals, are desired.

Commercially available Off-the-Shelf (COTS) and open architected hardware and software platforms should be used whenever possible, to reduce the DOC's dependency on any single provider, or vendors who have limited supply and support chains.

B. Differences - Facility Custody Levels

Washington State Department of Corrections classifies its correctional facilities according to a security level system, as follows:

- Level-5 Maximum Custody (Intensive Management, Administrative Segregation, Protective Custody, and other specialized population high-management units)
- Level-4 Close Custody
- Level-3 Medium Custody
- Level-2 Minimum Custody
- Level-1 Community Based, Partial Confinement

DOC facilities have their basic Housing Unit and facility perimeter construction and movement controls criteria defined in the Department's Custody Staffing Model (refer to Policy 400.020). Most institutions, and all complexes, are comprised of multiple custody levels. Housing Units with different custody levels may exist within the same perimeter, however, no Housing Unit may be used for a custody level higher than permitted by the facility's perimeter.

Most criteria in these Guidelines increase in complexity with an increase in facility custody level. Many of the parameters in these Guidelines will reflect a distinction in requirements for Security Systems which occurs between the Community/Minimum Custody (Levels 1 and 2) and the higher custody levels (Levels 3, 4 and 5).

C. Security Electronics Equipment Rooms

1. Relationship to IT Equipment Rooms

   a. Security Electronics Equipment Rooms will require many of the same characteristics as telecommunications rooms as defined by the WSDOC TDIS, including specific HVAC and electrical requirements. Another requirement for Security Electronics Equipment Rooms is connectivity to optical fiber backbone cabling for campus distribution and integration.

   b. The TDIS specifies a common or "shared" optical fiber backbone to support all electronic systems wherever possible, to reduce the installation and maintenance costs of physically separate campus distribution systems.

   c. In an effort to reduce overall costs and the space dedicated to providing support for electronic systems, the Security System Designer should collaborate early with the project RCDD to provide shared spaces or rooms serving the needs of both the telecommunications systems and the Security Systems. Should the Designer determine specific rationale for NOT providing shared

space for these functions, the Designer should make every effort to locate any dedicated Security Electronics Equipment Rooms in close proximity to the telecommunications rooms.

d. Specific space requirements are denoted below for spaces serving as a dedicated Security Electronics Equipment Room. Specific requirements for telecommunications rooms can be found in the TDIS.

2. Enclosure and Access Provisions

a. Based upon the critical function of these spaces, a secure envelope of physical construction is needed to restrict the potential for unauthorized access for any space housing Security System equipment and/or connections. Typically Security Electronics Equipment Rooms should be designed to have envelope construction (the walls, floor, ceiling/roof and any openings therein) equal to the highest security-rated construction used elsewhere in the building.

b. Room access doors should be hinged to open out wherever possible. It is desirable to have access to these rooms from the exterior or via mechanical rooms which have such exterior access; in cases where exterior access is not possible, doors should be carefully located to provide access via areas not regularly accessible to offenders.

c. All Security Electronics Equipment Room doors, including those shared with IT, should be monitored for security and must be fitted with doors, frames, and locks of a security grade commensurate with the enclosure walls, and with keying whose distribution among staff is highly restricted, but is consistent with DOC policy 280.310, to allow those with a legitimate need for access to have it.

d. Completely separate buildings or facilities may be constructed to serve as the campus main Security Electronics Equipment Room (SEER) and or the main IT distribution facility (MDF). When these services are provided from a dedicated facility, which may be located outside the secure perimeter of the facility, additional levels of security and access control may be required.

3. Supporting Systems and Environmental

The Security System Designer should provide to his counterparts on the design team a summary of the environmental requirements for the Security Electronics rooms no later than the beginning of the Design Development phase of the project.

a. Lighting:

Lighting should be a minimum of 500 lux (50 foot candles) measured 3ft above the finished floor. Fixtures should be a minimum of 8'-6" above the finished floor. Placement should be coordinated with racks and enclosures to provide the best lighting exposure, while maintaining adequate clearance from cable pathways and connection points to avoid electromagnetic interference (EMI). (See the TDIS for further definition of acceptable clearances from sources of EMI.) Emergency lighting is required within these spaces.

b. Electrical:

Security Electronics Equipment Rooms should be equipped with general purpose "convenience power outlets" and "technical power outlets". All outlets or connections providing power for the Security Systems should be powered from technical power outlets. General power receptacles should be used only for ancillary connections and should not be used to power permanent fixtures or equipment within the Security Electronics Equipment Room. The Security System Designer

should summarize the needs for electrical connections and outlets in the quantities required for the specific equipment being installed, and future needs.

In addition to the electrical connections required for specific equipment, the Security System Designer should apply the methodology denoted for power distribution in a telecommunications room as defined in the TDIS TDDG Version 5.2 Section 4.7.6. to any dedicated Security Electronics Equipment Rooms.

c. Mechanical and Fire Protection:

HVAC: Security Electronics Equipment Rooms should be designed to support active electronic equipment (hubs, routers, switches, file servers, etc.) even if the current design does not immediately call for such devices. The rooms should be provisioned with an HVAC system capable of operating on a 24 hours-per-day, 365 days-per-year, with no set back, to maintain a sustained operating temperature between 64-75°F degrees with a relative humidity between 30-55%. Humidity control (if required) should be integral to the HVAC unit or system; separate dedicated humidifiers should not be used. If the building system cannot assure continuous operation a stand-alone unit should be provided for the room. Typically a nominal 1-Ton dedicated HVAC split system is specified for these spaces, unless the anticipated heat load is greater than 1-Ton.

Piping: Wet piping should not be permitted in the room or space unless required by code.

Fire Protection: Main Security Electronics Equipment Rooms (rooms having equipment considered critical to operation of the facility as a whole) should have a clean-agent fire protection system (FM-200 or equivalent) in lieu of a wet system. Where fire suppression sprinklers are installed, the piping should be coordinated so as not to route directly above active electronics, and sprinkler heads should be equipped with wire cages to prevent accidental discharge. Where other solutions are not possible and wet pipes must be routed above active electronics, drainage troughs should be placed under the sprinkler pipes to prevent leakage onto the equipment within the room, but should not interfere with the required discharge head coverage.

d. Architectural:

The walls in Security Electronics rooms should be covered with ¾" thick A-C grade plywood backboards. The plywood should be painted on both sides with primer and two (2) coats of white, fire retardant paint, mounted with the A grade exposed. (The plywood should not be fire retardant treated type - paint tends to flake off of fire retardant plywood.)

Conduits in Security Electronics rooms will be permitted to be surface mounted. Security System Designer should detail the routing of conduits in this space to maintain as much usable wall space as possible (conduits should not be permitted to route in the middle of wall fields or dissect wall spaces that may be used in the future. Where backboards are applied to existing walls with existing power outlets and light switches, cutouts in the backboards should be provided for access to the existing electrical devices, with device box extensions installed as appropriate.

The walls and ceiling should be treated and sealed to eliminate dust. The floors should be light colored, slip resistant and equipped with static dissipative flooring to reduce risks related to static discharge to sensitive electronic equipment. Carpet is not acceptable.

4. Space Allocation and Clearances

The ANSI/TIA/EIA-569 standard provides a method for calculating the size of a telecommunications room based upon the floor area being served from that space. This standard is slightly modified

through the TDIS for the design of telecommunications spaces within DOC facilities, however it does not address specific needs related to security electronics. Based upon the similar nature of the services being provided from these spaces, the location and sizing criteria denoted in the TDIS should apply equally to a dedicated Security Electronics room.

When Security Electronics Equipment Rooms and telecommunications rooms are a shared resource, the formulas included in the TDIS for calculating the size of telecommunications rooms should be applied, with the overall sizing then being increased by 30% to accommodate the Security System equipment. This is to be considered the minimum space requirement, subject to verification and increase as follows:

- After determining the size of the shared space, the Security System Designer should evaluate the floor space available compared to the actual quantity of racks and other equipment to be installed.
- Provide capacity and dedicate space for future system expansion as well as capacity to support system upgrades and migration strategies for replacing equipment in an active environment. Typically a minimum of 40% additional space should be provisioned for this purpose. *Do not allow equipment re-configuration by the contractor to compromise this required dedicated space.*

When designing the layout for Security Electronics Equipment Rooms, the Security System Designer should provision adequate space for the equipment "footprints" as well as the clear working space that provides the ability to fully service, maintain, replace and install equipment into the racks or enclosures. Clear working space should be provided per the ANSI/EIA/TAI-569 standards as well as the requirements of the TDIS, but not less than the following:

- For equipment enclosures, the clear space in front of wall mounted enclosures should be no less than the greater of the width of the enclosure, or 36".
- Floor mounted enclosures should have front clearance not less than the total depth of the enclosure being specified (i.e. a 42" deep enclosure will require a minimum of 42" of clear space) to support installation and removal of equipment.
- Clear space behind or to the rear of floor mounted equipment enclosures should be no less than 36" where rear access is required for normal use or for maintenance.

All equipment specified for installation in a dedicated or shared Security Electronics Equipment Room should be securely mounted to the walls in enclosures, or be installed in floor mounted 19" equipment (server) rack enclosures.

D. Networks

1. Security System Network(s)

In line with the WSDOC's desire to create open architecture environments that are supportable and maintainable, the Security System Designer should employ native IP-based transport networks whenever possible. These networks may be standalone in nature, or integrated into larger infrastructures.

IP network transport devices as well as end devices located on any IP network (including stand-alone networks) should have IP addresses, with the address ranges and/or specific IP schema's assigned by DOC HQ/IT. Specific items that will be assigned by DOC HQ/IT include; network device names, IP schemas, V-LAN assignments and DNS information when required. The Security System Designer

should coordinate with DOC HQ/IT staff to identify those configurations and should be responsible for integrating those requirements into the design documents.

A diagram depicting the Security System LAN in its relationship to the other DOC Enterprise LAN's is included as an Exhibit at Section VIII of these Guidelines.

2. Network Access Points and Security

The Security System Designer should pay particular attention to restricting opportunities for access to the Security Systems network(s), to minimize risks associated with unauthorized connections.

Location of network ports, accessibility to functional PC ports, device authentication requirements, and other factors should be considered, with the risks appropriately mitigated in the design.

Dedicated modem lines, internet connections, ISDN, or other network access portals should not be configured, specified, or provisioned to provide Security System support without written authorization from DOC HQ/IT.

Where remote access to the Security System network is required, the Security System Designer should work with DOC HQ/IT to ensure that the approach specified to be available to the Security System Contractor is in compliance with DOC and ISB policies and requirements.

3. Systems Environment

All network transport devices, servers, storage arrays, and other head-end components of electronic security systems should reside in Security Electronics Equipment Rooms, shared Telecommunications / Security Electronics rooms, or spaces specifically designed to support the equipment being located there. These rooms and/or spaces should be provisioned as defined in this document, and according to the applicable requirements of the TDIS.

E. Owner Furnished Services and Hardware

1. Owner's Network Design Services

Security System Designer should consult with DOC HQ/IT representatives to determine the specific network design parameters that must be met, based upon the specific solution being designed. DOC HQ/IT typically provides the network transport layer design to support current or future integration into the enterprise network.

The design services provided by the Owner typically include physical design of the switching infrastructure including switches, routers, and firewalls, to include manufacturer, part number and software configurations. In addition to the transport hardware, DOC HQ/IT will assign the IP address schema, and the V-LAN strategy and assignment.

Based upon the procurement method (see "hardware furnished by owner" sections below for more information), the actual configuration of hardware may be performed by DOC or the Security System Contractor.

2. Hardware to be Furnished by Owner and Installed by Owner or Contractor

DOC HQ IT has in place contracts for the procurement of certain computing and network hardware. At the time this document was prepared, DOC maintains purchasing agreements for Cisco LAN and WAN transport equipment, and has separate leasing agreements for PC workstations and servers. It is the preference of DOC to directly procure as much of the computing equipment related to these systems as possible, to maintain continuity throughout facilities, and to streamline the support processes.

The Security System Designer should coordinate with DOC HQ/IT to determine the most cost effective and beneficial procurement method for these devices as it relates to the specific project's needs.

The procurement method for this equipment is vital to determining and controlling the long term costs of computer and network equipment associated with Security Systems, as the replacement of this inventory is generally managed at the HQ level. Network and computing devices not procured through this method will require additional consulting and provision of advisory information by the design team to educate the facility regarding the short and long term operational costs to maintain, update and replace these devices.

In addition to the design assistance and actual procurement of system hardware, the Owner may also provide installation for some or all of the devices procured through HQ/IT. Determining the responsible party for installation of each component and the sequencing of these activities should be completed during the design phases of the project, and communicated to potential bidders through the construction documents. The Security Systems Designer should work with the stakeholders to determine the critical path for the installation and configuration of this equipment and communicate those requirements to the project team during the construction administration phases of the project. Overall project schedule, timing, and prior testing requirements will be factors in determining the best approach to installing these devices.

In many cases DOC HQ/IT will physically configure, install, and connect the network equipment. However Security System PC workstations and servers may require substantial custom software, installation, program development, and pre-testing that would require a coordinated transmittal of owner-procured hardware to the Security System Contractor. This will be on a schedule well in advance of the site readiness for installation of the balance of the network equipment.

Delivery of all furnished-by-owner installed-by-owner equipment will be directed to the Local IT staff. Delivery of all furnished-by-owner installed-by-contractor equipment will also be to the Local IT staff for receipting and inventory purposes, and then transferred to the Security System Contractor through the general contractor, with a transmittal or other written document denoting the specific equipment delivered. (In the case of a new facility where Local IT staff may not yet have a presence or facilities the Security System Designer should confirm with the DOC project manager the delivery and transfer scenario.)

F. System(s) Integration

Security system integration is a required feature for all DOC projects. The degree of integration may vary, depending upon, for example, operating legacy systems where the project is expansion of existing facilities. The Security System will integrate the sub-systems and field devices into a networked programmable logic controller (PLC) based control and monitoring system. The PLC will be pre-programmed to meet the requirements of these Guidelines, and as further determined by each project's stakeholders.

1. Required Integration

The Security System should

- Make use of an appropriate hierarchical annunciation logic, which notifies the appropriate staff of selected events.
- Provide for overall project area control from the designated Master Control space.
- Provide for local control at designated Control Points as determined during design.

- Provide time synchronization across all sub-systems, in conjunction with accessible, searchable, and secure event and activity logging to a SQL database. These provisions require integration at the software level by the Security System Contractor.
- Systems Integration to Human-Machine-Interface (HMI) Control Points should include the following sub-systems:
  - Door/Gate controls, which may include provisions for interlocking
  - Door/Gate status monitoring
  - Duress switch monitoring
  - Intrusion detection device monitoring (within secured rooms, etc)
  - Video system standalone for system management (including archival storage) but integrated for switching associated for movement/door control and surveillance
  - Audio security system (intercom) switching associated with door/gate control point-to-point 2-way communication
  - Audio system switching for paging
  - Perimeter Intrusion Detection System is standalone for system control, but associated to the PLC/HMI for alarm annunciation and video switching
  - Water supply control for higher level facilities
  - Lighting control for cells and dayrooms
  - Offender telephone and JPAY cutoff
  - Staff telephone and administrative LAN cutoff
  - Entertainment television cutoff

2. Optional Integration and Feature Utilization

   Access Control systems as may be included in the project and doors/gates controlled by the system may or may not be integrated to the PLC/HMI for status monitoring and take-control provisions.

   DOC may incorporate audio recording capabilities at selected areas of a facility. Reference to DOC Policy 420.450.

   Paging integration to the facility telephony system may be considered as a means of providing multi-point Master access to the system for announcements.

   Video motion-detection as a means to detect intrusion in restricted areas can be considered for specific applications.

3. Undesirable Systems Integration and System Capabilities

   DOC does not utilize audio-level monitoring capabilities, as may be an available feature in some intercom systems, to identify a condition which would initiate an alarm.

   Undesirable systems integration includes any integration of the Security System with:

   - Fire alarm systems
   - Environmental (HVAC) systems control (except special cases as noted herein below)

G. Perimeter & Facility Entry / Exit Points

1. Perimeter Intrusion Detection

   A double-line fence with the inner fence having a Perimeter Intrusion Detection System (PIDS) for detection of attempted escape is required for the entire perimeter of Level-3, Level-4 and Level-5

facilities. Level-5 housing contained within a facility having a Level-3 or Level-4 perimeter need not have detection on its interior separation barrier if the facility perimeter meets these requirements. These Guidelines discuss only the PIDS and its integration with other parts of the Security System – not the other attributes of the perimeter enclosure.

The PIDS should provide

- A very low False Alarm Rate (FAR)
- A very high Probability of Detection (POD)
- Immediate detection and annunciation
- Minimal system maintenance requirements
- High system uptime without failure

The design should carefully consider the facility layout and provide seamless, but zoned, coverage. Pay particular attention to any junctions between the perimeter and buildings, the junctions of interior demising fences with the perimeter, perimeter corners, gated openings, changes of slope or grade elevation, etc.

2. System Control and Management

The Perimeter Intrusion Detection System should have its own Alarm and System Management PC, which should have a GUI containing a 2D or 3D representation of the facility and the perimeter zones, which should be identified and indicate status. This PC should normally be located at Major Control. The operator privileges should be restricted to allow only day-to-day system activities.

Penetrations of the perimeter should be sallyports, and the detection measures at each should be on a separate zone, allowing interruption (bypass) of only that gate's zone at periods when access through the perimeter is allowed, while maintaining detection in all other zones. Bypassed monitoring should be indicated on the screen in steady "yellow".

Other system actions, such as adjusting settings, troubleshooting, etc are restricted by log-on privilege to Electronics Technicians who will normally access the system at the Security System Maintenance/Administrative Workstation PC.

The system should maintain a time-stamped electronic log of events, including each alarm, alarm acknowledgement, alarm and zone reset, zone bypass, system troubles, etc.

3. Alarm Annunciation

Detection should be zoned such that the location of any perimeter breach attempt can be identified. Alarms should annunciate visually on the System Management PC's screen with flashing "red" zone indication on the map and audibly with a tone.

The system should be integrated with the Security Video System such that detection zones are associated with cameras which provide a view of the entire in-alarm zone and the immediately adjacent zones (3 zones total), when a zone is selected from the GUI, or when an alarm is acknowledged. Refer to "Security Video System – For Perimeter Surveillance and Alarm Association" in this Section, for further details. Video monitors for display of those views should be located at the Alarm and System Management PC.

Verify with the facility if mobile or remote system status and alarm receivers are desired, and if so, the number and type to be provided. If an RF transmitter is used in conjunction with the system and which

requires a radio transmitter license, begin coordination early with the Agency's Federal Communications Commission (FCC) License Coordinator. Only the Alarm and System Management PC will be able to reset alarms or change the status of system zones.

H. Access Control Systems

1. Application

Automated access control may be employed to provide a keyless means of access to administrative areas or similar facilities located outside of the secure perimeter of facilities. Use of automated access control is subject to DOC establishing operational policies similar to its key control policies.

Access Credentials are unique and also serve as the DOC staff person's identification badge. Credential format must be compatible with the Owner's badge printing process. Access Credentials may also be utilized for an Automated Accounting for Personnel system, as discussed below. Credential format should be verified to assure compatibility with all subsystems.

2. System Features

Access privileges will generally be assigned in a managed scheme where persons needing access have the privilege and those who do not are denied access.

Access control is normally deployed at an opening with a door or other barrier, and may be one-way with "free" return access via Request-to-Exit (REX) sensor (hardware or electronic), or two-way where the Access Credential must be used for access and return passage. In cases where positive control without tailgating is needed, consider the use of turnstiles (either electronic type with suitable barriers to circumvention, or full-barrier type allowing only one individual to pass).

I. Automated Accounting for Personnel Inside the Perimeter

At the time of development of these Guidelines the Department of Corrections is undertaking a study of means and methods for determining at any point in time the identification (and to a degree yet to be determined the location) of all staff, volunteers, visitors, vendors, contractors, and others (not to include offenders, who are subject to a stringent accounting), who are within the facility's perimeter. This subsection of the Guidelines will be updated to reflect the Agency's requirements in that regard.

J. Control Points

1. Custody Level Distinctions

Control Points are, for the purposes of this document, any location where supervisory monitoring or operational control of a Security Video System, facility doors/gates, an intrusion detection system, or any other Security System devices, occurs.

Level-3 and higher facilities will have staffed Control Points which may include Major and Minor Control Rooms, Housing Unit Control Booths, Movement Control Booths, Towers, etc. Such Control Points are to be established only within environments having adequate barriers against forcible entry.

Level-1 Community Based / Partial Confinement and Level-2 Minimum Custody facilities will not have Control Rooms or Control Booths, but will have a central Duty Desk or Security Station from which staff monitors and performs limited control and monitoring of the facility.

2. Major Control

   The Control Point which is designated for handling the highest level of facility control and monitoring, and which receives and manages radio duress and perimeter alarms, is usually designated as Major Control. In newer facility designs Major Control is located outside of the facility perimeter, and may have only limited direct vision of the facility interior. Major Control should normally be configured to:

   - Control movement through the perimeter, by pedestrian and vehicular (unless the site is configured with a Tower providing) sallyport gate control
   - Control and/or monitor of exterior openings for all buildings on the facility grounds (inside and outside of the perimeter, as determined)
   - Assume the control and/or monitoring duties of any other Control Point in the facility.

   Major Control is normally configured with more than one (1) Control Workstation. The quantity required is dependent upon the workload forecast, and is usually configured to allow for a variable staffing level where fewer Workstations are staffed at lower activity periods, and more are staffed at peak periods. The operational configuration typically provided is for all Workstations to receive all alarms and calls from Major Control's area of control. Thus, any Workstation can answer any call or alarm, or perform any system operation which is not restricted to supervisory level operators.

   One (1) Workstation may be configured as a "training" station, for new operator training.

   Major Control should have the PIDS Alarm and System Management PC for perimeter alarm annunciation and control.

   Major Control should have access to live video from any camera on the facility site. It may have a Video Workstation that is configured for archive video review and export.

   Major Control should be able to connect by intercom to any Control Point, and page to any paging zone on the facility site, including the capability for "all page".

3. Minor Control, Movement Control Booths, and/or Towers

   Minor Control, Movement Control Booths, and Towers may have monitoring and control of designated doors/gates, and are to be configured similarly to Housing Unit Control Booths.

4. Housing Unit Control Booths and Limited-Control Panels

   Housing Unit Control Booths are provided in Level-5 Maximum Custody and Level-4 Close Custody housing units. Level-3 Medium Custody housing units may have limited control and monitoring panels only. (Level-2 Minimum Custody and Level-1 Community Based / Partial Confinement units usually will not have any control or monitoring in the housing unit.)

   Housing Unit configurations vary, but careful thought should be given early in systems design to opportunities for "virtual consolidation", whether by reducing the number of Control Points within a Control Booth that have to be staffed, or by transfer of control of housing sub-units (pods) or entire Units to another Control Point, during periods of low Unit activity and movements, and/or for relief backup. Scenarios commonly used to achieve this flexibility are:

   - Two or more Control Points in the same Unit or Booth have the same screens and "mirroring" each other, with all receiving any calls and alarms, and allowing any of them to handle any event or task for the areas collectively controlled;

- A “transfer-of-control” methodology where control is given up to another pre-determined Control Point, which may be another Housing Unit or Booth within a Unit, or to Major Control.

Housing Unit Control Booths should have local internal control of the Unit, and should monitor status but not receive alarms from, or control doors and gates comprising the Unit exterior, including roof hatches and the like. Control of entry or exit from the Unit is normally delegated to Major Control (ie: if a Unit has a sallyport entry, the exterior door is controlled by Major Control, the inner door is controlled by the Housing Unit control panel with an interlock preventing either from operating their door if the other door is not secure).

The Housing Unit Control Booth operator should have access to live video only, and only the video originated within the Unit and its immediate exterior approaches and directly associated yards. Limited-control panels are not provided with video monitors.

Housing Unit control panels should provide for paging to the available zones within the Unit, and for intercom connection to Major Control.

Cell lighting control should include the ability to force cell lights “on” or “off”, and the ability to turn on “count” lights. Dayroom lighting should be controllable from the panel to provide variable levels of artificial light, but never a dark room.

Level-4 and Level-5 Housing Units will have complete control over cell doors, which will be sliders, Dayroom entry doors, also sliders, and all other controlled doors in the Unit. Level-5 cell doors will have a “door enable” switch at the non-cell side of the door which must be pressed and held to enable opening the cell door. (This is a safety feature to prevent operation of a door other than intended, or operation of a cell door when custody staff is not present and ready to remove the offender from the cell.)

Level-3 Housing Units have no local unlocking controls, and will be configured with two modes of (swing) cell door operation:

- “Offender-Control” mode, where the offender may use a standard key in an electrical keyswitch on the Dayroom side of the door, or activate his in-cell intercom switch to electrically operate the lock; and,
- “Staff-Control” mode, where the keyswitch remains functional but the intercom switch no longer unlocks the cell door, becoming a standard call button. Under “Staff-Control” mode all cell door unlocking is from a secure Control Point (Major Control or as designated – never to the local limited-control panel) under an operational protocol that provides for the local Unit staff to be aware of the planned unlocking. Intercom calls from the cells go to the local limited-control panels, and if not answered go to the secure Control Point.
- The change of “mode” from “Offender-Control” to “Staff-Control” may be invoked from the Housing Unit’s limited-control panel, but changing from “Staff-Control” to “Offender-Control” can only be invoked from a secure Control Point (such as Major Control).
- All door locking control is through the PLC, never directly to the lock or operating device.
- Controllable cell doors should individually be provided with a “lockout” mode, invoked at the control panel as a “toggle” which when enabled prevents electronic unlocking of the cell door. Connection to the cell’s intercom station is possible. The cell door is removed from any group-unlock actions except emergency egress. Removal of the “lockout” mode restores the capability for unlocking the cell door individually, or if it is a member of a pre-assigned group.

Controllable cell doors in Level-3, Level-4, and Level-5 Housing Units may be organized into pre-determined groups for group opening/unlocking, as determined by the facility. It may be desirable to provide for operator-assignable grouping capability (say for creating a group of cells to be released for work assignments).

In Level-3 Housing Units some movement doors may be configured to allow them to stand open or remain unlocked for long periods of time without causing an alarm, to facilitate frequent offender movements as regulated by Unit staff.

In all Levels provisions must be considered in the design for emergency access and emergency egress.

- Emergency access must consider
  - The "loss of control" due to a security system or system component failure
  - Provisions for overriding door interlocks to move emergency response forces and equipment through controlled sallyports
- Emergency provisions for
  - Initiation and annunciation of "duress" alarms from selected locations
  - Safe and secure egress of building occupants to appropriate areas of safety, which may include group-release of sets of cell doors, automated removal of restrictions on cell door opening
  - Making security systems inoperative locally, and the initiation of alarming for the case of staff needing to vacate the Control Point
  - Restoration of local control, post-event

K. Touchscreen HMI

1. HMI Attributes

General: The Human Machine Interface (HMI) software should provide a graphical user interface (GUI) which facilitates operator actions, and provides visual indication of the status of the doors/gates/devices making up the Security System. Consistent use of icons and the color scheme throughout the screens should be employed to promote ease of training and usability. Selected icons should change appearance and be associated with a soft "click" sound upon being touched as a means of providing user feedback. Control icons that are unavailable for selection should be displayed in a manner that indicates that status.

2. Screen Organization and Operations:

All Security System screens should be consistent in appearance and operation. Example screenshots from a touchscreen control system is included as an exhibit to these Guidelines, at Section VIII.

- All screens should have a "Toolbar" with selectable titled icons. The "Toolbar" will remain visible in all screens. A single touch selection of a Toolbar icon momentarily changes (animates) the icon state as if a real pushbutton has been pressed, and brings up the associated screen, control icon group, or the alarm or call event from the queue.
- The screens will also have the current time and date displayed.
- The large working area is reserved for facility maps, auxiliary device status and control icons, etc.
- Provide map screens utilizing accurate scaled building floorplans

- Maps should be oriented in proper visual relationship to the operator's location in the facility
- Organize screen layouts to provide proper size and separation of selection icons, but minimize the number of separate screens required.
- Provide navigation tools on map screens that take the operator to adjacent areas and provide for navigation between all available screens with a minimum of "touches" or mouse clicks.
- "Touches" or mouse clicks should annunciate with a soft "click" sound to confirm system acceptance

3. Queues:

Provide for separate Queues for Calls and Alarms on each screen. (Panels controlling small Housing Units or a limited number of doors/gates may have a combined Call and Alarm Queue, as in the example Touchscreen screenshots.) They should have space for at least five (5) events to be visible in each. The Queues should have a capacity of at least 1,024 pending events each.

- Queues should always be available (except during "screen clean" or "calibration")
- Only alarms and calls from the areas/devices being controlled and monitored on that control panel should be annunciated. Some panels may operate as "mirrors" of other panels
- Queue events are FIFO for calls, LIFO for alarms, except that duress alarms are priority alarms over all other types of alarm
- Alarms and call events should have device type and location identification text displayed in the Queue
- Alarms will display in the Queue with red text descriptor; calls display with yellow text, both contrasting with the background.
- Alarms and call events can be selected from the Queue (any displayed event line) or directly from the maps by selecting a device control icon which is indicating a call
- Provide for operator selection by "next" (first unanswered call, or most recent/highest priority alarm), selection of any event line in the visible Queue, or "previous" (which will return to the last event acted upon, with its associated map screen displayed and the device selected). The "previous" buffers should contain at least eight (8) events, ordered most recent to oldest.
- Call/alarm selection from the Queue automatically brings up the map screen of area where the device is located, if not the current screen, and selects the device.

4. Colors:

Color schemes employed should provide the proper level of visibility without glare, and promote the ability to distinguish between elements, and be selected in color ranges "easy" on the user's eyes.

- "Red" will always indicate an insecure condition or an alarm condition. In the Alarm Queue this indicates a pending alarm event in the panel's controlled and monitored areas. Red background in text boxes may be used to indicate very important warnings to the operator.
- "Green" will always indicate a secure "normal" condition.
- "Amber" will always indicate a condition where monitoring or control by the panel is temporarily inhibited (due to an interlocked door being non-secure, an alarm being bypassed, or a time schedule or operation mode change, such as "lockout" mode being set).

- Door/gate interlocks should be graphically indicated on the screens (amber) when any door in the group is not-secure. The indication should have graphical links between the interlocked devices connected to an "I" within a circle.

- "Yellow" will always indicate a pending call at a device. In the Call Queue this indicates the panel has a pending call event within its controlled area.
- "Blue" will always indicate the currently selected and active device(s) and device control icon group.

5. Status Icons:

   Status icons are separate from Selection Icons and indicate the "realtime" status of doors/gates (secure / not secure), including doors/gates on the screen which are not controlled. A concentric ring surrounding the status icon indicates the "realtime" status of monitoring of that device. Graphical indication should be based from PLC state change of the monitored device – not as "forced" in the Graphical User Interface (GUI).

   - A red filled-circle icon indicates a door/gate/device that is non-secure
   - A flashing red filled-circle icon indicates a door/gate/device that is in-alarm
   - A green open-circle icon indicates a door/gate/device that is secure (locked, closed)
   - A steady red concentric ring surrounding the status icon indicates that monitoring is disrupted (device is non-secure); a flashing red ring indicates a device that is in-alarm and has not been reset
   - A steady amber concentric ring surrounding the status icon indicates that monitoring is inactive (bypassed)
   - A steady green concentric ring surrounding the status icon indicates that monitoring is active
   - Icons should not flash or otherwise animate, except as described.

6. Door/Gate/Device Selection Icons:

   Selection Icons are to be provided in a "square" button shape with text labels.

   - Icons indicate a call pending at a door/gate/device (intercom) by a yellow concentric square-corner frame surrounding the Selection Icon; a call initiates a single chime tone at the touchscreen.
   - Icons indicate the currently selected door/gate/device by a blue concentric square-corner frame surrounding the Selection Icon; de-selection is by a second touch/click, by selection of another event from the Queue or another door/gate Selection Icon, or selection of the "cancel" control icon in the Toolbar.
   - Text should be the (Owner's system) cell number, door number, room reference name, or as approved.
   - Device Selection Icons should be provided for:
     - Doors/gates in combination with their associated intercom stations or call switches and monitoring devices (all to be represented by a single device selection icon). An intercom station located to be shared by two doors/gates is associated with both,
     - Non-associated intercom stations and call switches,

- Non-associated monitored devices,
- Paging zones,
- Controlled utilities (water, power, lights, HVAC, etc) (provide one device Selection Icon for each controlled device or selectable operation),

Initiate "listen" mode intercom connection automatically when a door/gate with intercom stations or an intercom device Selection Icon is selected.

7. Control Icons:

   Provide appropriate Control Icons organized in groups associated with the selected door/gate/device components (i.e. Control Icons for swing doors should provide only unlock function; Icons for slider doors should provide for opening, stopping, and closing; Control Icons for doors held unlocked should provide for re-locking; and so on), and only the various icons in the Control Icon group will be selectable dependent upon the device status (i.e. if the slider door is opening the "open" icon is not selectable, but the "stop" and "close" icons are).

   Provide "push-to-talk" function as a Control Icon when a door/gate has an intercom station. Either the icon, as a virtual switch, or the physical switch on the microphone/speaker unit, may be used for the "push-to-talk" function.

8. Tones:

   Audible "tones" are to sound at the control panel for calls, door/gate alarms, duress alarms, and system malfunction alarms.

   - Calls sound only one (1) time until selected, regardless of the number of times the call initiation button is pressed.
   - Alarm tones are continuous and can be silenced after event selection from the Alarm Queue or device selection. Silencing does not reset the alarm – a separate step is required. Alarm reset cannot be accomplished until the door/gate/device is re-secured or physically reset.

9. Control Panel Duress:

   Provide in the Toolbar an always available icon to initiate the multi-step Control Panel Duress function.

   - Initial selection of the function should activate a large pop-up having a red background textbox and icons provided to "Confirm Duress Shutdown" or "Abort". A clearly worded text warning to the operator that confirming will initiate a process shutting down the process and sending an alarm to Major Control is to be provided.
   - If aborted panel operations will continue as usual. Confirming will bring up a final pop-up having a red background textbox and icons provided to "Send Alarm & Shutdown Panel" or "Abort". A clearly worded warning in large text will advise that this is the final step – the Panel will shut down and the alarm will be sent if confirmed.
   - If aborted panel operations will continue as usual. If confirmed the panel will be shutdown and become inoperable, and all video monitors at the control point will be powered off. If the control point is a Housing Unit all cell water valves will be turned off, the offender telephones and JPAY system will be disabled, the staff LAN and telephone system will be disabled, and all control will transfer and a priority duress alarm will be transmitted to Major Control. Systems re-starting and re-activation requires technician and maintenance staff actions, and cannot be restored by Major Control.

10. Additional Requirements:

    The touchscreen HMI is dedicated to Security System monitoring and control and shall have no other operational programs.

    - A keyboard should not be required for operation, and should not be installed. (Note: An exception would be for database applications where operator inputs needing a keyboard are specified.)
    - A standard optical mouse without a wheel or extra buttons should be provided, which has the same functionality as the touchscreen, using the left button for "pick" selection. Other buttons should have no function assigned.
    - Except for the special Control Panel Duress operation there should be no user access or commands available on the touchscreen, or by mouse, that would invoke either a system shutdown/reboot, or an operating-system level function, such as starting or stopping a software program or process.
    - Following a technician's system re-start after Control Panel Duress (or on system failure), to the extent possible, control system programs and screens should auto-load to the user log-on or Main Screen.
    - There should be no "screensaver" or screen "power-save" functions enabled, unless associated with a "timeout" function intended to disable a control panel that may not be always attended.
    - Provide a means for "screen cleaning" - the screen displays a timer countdown for a (program adjustable) period during which the system does not recognize screen "touches" or mouse clicks.
    - Touchscreen calibration routines should provide a means to abort, to ensure immediate control availability.

L. Security Video System

1. System Design

   It is the intent of DOC to move towards a facility-wide fully digital to-the-edge Internet Protocol (IP) networked video system with network archival storage and virtual matrix switching that allows for network-wide viewing of live and archived video.

   Legacy all-analog, or analog with Digital Video Recorder, systems should be transitioned toward this goal, and Hybrid Video Recorders (HVR's) should only be used on a case-by-case basis, with such use to be proposed as an Alternative to these Guidelines.

   The Security Video System will operate over the Ethernet security system network and be interfaced to the PLC/HMI control system.

   NOTE: At the time of writing these Design Guidelines the Department of Corrections is beginning an effort to establish Standards for Security Video Systems in its facilities. The Guidelines will be updated to reflect the Standards adopted.

   Design parameters for Security Video Systems:

- The facility staff should perform, during facility design, a Risk Assessment to determine the interior and exterior areas requiring video surveillance, and the degree of acuity required in each area
- The required coverage should be achieved using fixed cameras
- The Risk Assessment should determine which areas require pan-tilt-zoom capability for supplemental surveillance (pan-tilt-zoom cameras should NOT be used for primary surveillance)

2. For Perimeter Surveillance and PID Alarm Association

   Level-3, 4 and 5 facilities should have video surveillance of the perimeter, organized so that coverage coincides to the detection zones. Reference to paragraph G. of this Section, above, for integration with the PIDS for by-zone camera call-up, and alarm acknowledgement association.

   Use of pan-tilt-zoom cameras for this coverage should be avoided due to the requirement for coverage of multiple adjacent perimeter zones simultaneously.

3. For Movement Control

   Every controlled door/gate in facilities of all custody levels should have cameras of a type and at a location on both sides of the opening to provide for positive facial identification of persons requesting movement. (Doors/gates which may have direct line-of-sight from the Control Point are generally not exempt from this requirement, unless it can be predicted with great certainty that control will *never* be transferred to another remote Control Point.)

   Programming of the Human-Machine Interface (HMI) or PLC associates the cameras with the door/gate controls for automated call-up display.

4. For Surveillance

   Surveillance requirements for areas within the project scope should be determined by the Owner's facility staff following a comprehensive risk analysis exercise. General guidelines include:

   - Interior or exterior areas where offenders congregate, move, and work or program in groups of two (2) or more, are likely to require comprehensive fixed surveillance camera coverage.
   - Areas where offenders recreate, eat, and visit are likely to require supplemental pan-tilt-zoom camera coverage.
   - Special purpose cells may require coverage.

5. Cameras

   Locate cameras:

   - With consideration for sources of glare or extremes of light level,
   - Out of the reach of offenders, or if unavoidable, in suitable housings.

   Camera placement and/or image masking should preclude viewing specific areas where offender privacy is recognized (showers, toilets).

   All cameras should be represented on the HMI with graphic icons which indicate the view direction and camera ID number. Pan-tilt-zoom cameras should have icons indicating that capability.

Pan-tilt-zoom cameras should have a "home" position pre-programmed by the Security System Contractor which is to an easily recognized view.

6. Recording

Recording of video data will be continuous for all cameras, with the archiving to meet the performance and retention requirements established in these Guidelines. Recorded video data may be used for evidentiary or forensic purposes.

7. Live Video Viewing

Control Points having movement control functionality should have live video viewing capability for all cameras originating in their area(s) of control. Except for Major Control, cameras located in other areas of the facility should be unavailable. Viewing of archived video should be unavailable at Control Points.

Control Points having movement control functionality should have no fewer than two (2) monitors:

- One (1) is configured for quad-view, to be used for automated movement door/gate call-up video display, but is also assignable for surveillance use by selection of camera icons from the HMI and assigning them to an icon representing the monitor's display quadrants.
- One (1) is fully configurable by the operator as to number of images displayed, the display configuration, and which cameras are viewed.

Control Points having large areas of control, and specifically Major Control, should have additional monitors to allow for greater live-view surveillance capabilities, with the control operator(s) able to set viewing configuration and assign cameras to viewports.

Limited-control Control Points will normally not have video monitors.

8. Archive Video Viewing

Archive and Live Viewing capable video viewing Workstations should be provided as required by the scope of each project, but generally are provided in the Shift Office, Investigations and Intelligence offices, and in the Emergency Response Management room.

9. System Expansion

The Security Video System should be configured in hardware, and provisioned with software capacity, for cost-effective expansion by adding cameras and incrementally increasing the video management servers and archival storage capacity.

M. Audio Systems

1. Intercommunication

The digital intercom system should have station devices with 2-way speaker-microphones and call buttons located at each movement door/gate, within each cell or dormitory, and at other locations as determined. The system will have Master stations at each Control Point, and in other locations to be determined.

The stations will be integrated through the PLC/HMI programming so that calls initiated from the station will annunciate at the appropriate Control Point, and selection of the call, or in the absence of a pending call, selection of the door/gate associated to the station, will connect an audio channel between the Master station and the intercom station. The system should allow for multiple remote stations to be connected to a Master. The Master automatically connects in "listen" mode with push-to-talk available;

the remote station is hands-free. Some areas (requiring confidential conversations) may require provision of a tone at the station to announce the connection.

The system operates on the Ethernet security system network, allowing audio communication between any station and remote Master stations under a transfer-of-control scheme.

2. Paging

Paging is provided to facilitate communication from staff to selected portions of the facility, which can be interior or exterior. The zoning of the paging systems should be determined during design. Consider use of two-way (talkback) paging in smaller interior zones.

Paging can be initiated from Control Points using the HMI for zone selection, or from Master stations having zone selection capability.

N. Security System Maintenance/Administrative Workstation

The Security System should include a Maintenance/Administrative Workstation, to be located in a suitable, secure area with restricted access. The Workstation should have a large LCD monitor, keyboard and mouse, with software and a KVM switch or other configuration that permits it to access and remotely manage all Security System servers and workstations on the network.

O. Auxiliary Devices / Systems Control or Monitoring

1. Duress Initiation Switches

Fixed-point duress alarm initiation switches of a type requiring physical resetting after actuation should be provided at areas of the facility where the Risk Assessment has determined a need for staff or volunteers to be able to initiate an alarm to the control panel which has monitoring and control of the area. The duress switch is continuously monitored, and a duress alarm is a priority alarm, whose location should be annunciated on the panel.

Switch locations should take into consideration the room shape and furniture arrangement, to maximize switch access opportunity in a stressful situation that could include physical confrontation. Consider provision of a visual indicator light to assist responders in locating the origin of the alarm.

2. Intrusion Detection Devices

Interior spaces where weapons, special equipment, tools, or sensitive information are stored may require supplemental monitoring for intrusion, in addition to entry door monitoring. Appropriate technology, such as Passive Infrared (PIR), Doppler Microwave, glass-breakage sensors, etc. should be employed. Alarms should annunciate to a 24/7/365 staffed control point, typically Major Control.

3. Water Control

Water supply system controllable (solenoid type) valves should be included in the mechanical design to provide for shutoff of plumbing fixtures in Housing Unit cells. This feature provides a means to reduce flooding impacts, and to prevent flushing of contraband in advance of cell searches.

- In a Level-5 Unit control should be provided for each group of cells served by a common chase. For example: In a 2-tier scheme with the cell pairs having a combination sink/toilet fixtures backed up to a common chase, provide isolation control for the four (4) cell group; Also provide a single selection icon in the HMI for control of the water supply to all of the fixtures within a pod.

- For Level-4 Units isolate logical cell groups, which should not exceed twelve (12) cells in any group; Also provide a single selection icon for control of the water supply to all of the fixtures within a pod.
- In Level-3 wet-cell Units isolate logical cell groups which are not larger than 32 cells per group. If more than four (4) controls per pod are implemented provide, in addition to the groups, a single selection icon for control of all valves serving the pod.

The controls should be implemented in the control panel HMI as "toggle-on" and "toggle-off", with valve status indicated. (Note: Valve status monitoring is not required – indication is the panel's control status only).

4. Lighting

Lighting systems in Level-3 and higher Housing Units should be controlled through the control panel HMI. The Security System should be interfaced with the lighting controls so that:

- The Dayroom lighting scheme provides for variable lighting levels by switching ON/OFF selected fixture groups via the control panel HMI,
- Cell "count" lights are controlled ON/OFF as a group (a tier or a pod as determined by facility staff) from the HMI.
- Level-5 cells are controlled by DOC staff from a standard switch located outside the cell – the control panel can force ON/OFF any cell's light individually.
- Level-4 or Level-3 cells will have control of their own light from a standard switch inside the cell – the control panel can force ON/OFF the cell lights as a group (may be a tier, partial tier, or as determined by facility staff),

The above described controls should be implemented in the control panel HMI as "toggle-on" and "toggle-off" for each function, with status indicated. (Note: Indication is panel control status only).

5. HVAC

Within Level-5 Housing Units (only) provide an interface to the HVAC control system for the housing pods to initiate operational modes established in the HVAC controls which support custody operations. The Security System Designer should coordinate provision of these features with other members of the design team as appropriate.

Each Pod within a Housing Unit should be individually controllable, to have:

- A mode which, when invoked, prevents the spread of O.C. (oleoresin capsicum) pepper spray or other agent to other Pods or areas of the Housing Unit during and after its application,
- A mode to expedite removal of the agent from the Pod after application and resolution of the incident, and
- A mode for HVAC shutdown to assist in overcoming a disturbance.

HVAC systems should not otherwise be integrated with the Security System, since the HVAC controls for normal purposes are determined by building and life safety codes, and environmental considerations, rather than by security considerations.

6. Offender Telephones and JPAY®

   In all Housing Units, controls and systems interfaces should be provided to cut-off offender telephone lines and JPAY® system access.

   For Level-3 and higher Housing Units cut-off is to be initiated from the control panel, but service restoration requires reset by technicians. Cut-off should be automated with the Control Panel Duress disabling of the control panel.

   For Level-1 and Level-2 Housing Units the cut-off may be by manual switched means (confirm switch location with facility staff).

7. Staff Telephones and LAN

   In Level-4 and Level-5 Housing Units, control facilities should be provided to cut-off staff telephones and the administrative LAN (to be used in case of offender takeover of the Unit). This control should be automated with Control Panel Duress disabling of the Housing Unit Control Booth panel(s).

8. Device Status / Health Monitoring

   Status/ health monitoring should be provided in the Security System, with status indication and fault alarming on both the local control panel HMI and the Maintenance/Administrative Workstation, for at least the following sub-systems and devices:

   - Digital intercom
   - Ethernet transport devices
   - UPS devices
   - PLC's.

P. Staff Duress Alarm System

The Agency, at this writing, is conducting a separate focused effort for the development of its Guidelines for a Staff Duress Alarm System to be deployed in its facilities. This Section will be updated following the conclusion of that effort.

Q. Relational Databases

The Department of Corrections desires to leverage the information contained in its databases to enhance security and safety. Present day schemes have been limited in their ability to integrate existing data with the Security System due to the physical separation of the networks, so it has not occurred, with the following exceptions:

- There has been beneficial use of a relational database where certain data (offender photos) is exported from its source and imported onto the Security network, then matched with cell assignments as an aid to the control panel operator for verifying identity and granting appropriate cell access. This system is capable of managing cell/bed assignments, identifying bed vacancies, and generating other management reports.
- There has also been a database application employed for all Level-5 Intensive Management Units (IMU's) which uses a standalone database to organize and associate offender's management data, track his activities and whereabouts, record staff interactions and activities related to the offender, records the issuance of articles to the offender, record results of cell searches, and many other events normally recorded in logs. This system is capable of

generating reports for supervisory review, documentation, and analysis purposes. The Security System is configured with a separate monitor, keyboard, and mouse for normal data input from pre-configured menus, but with provisions for entry of text notations.

V. Quality and Performance Requirements

A. Servers and Workstations

1. Operating System Software

a. Products and Versions
   1) Operating System software shall be reviewed with DOC HQ IT by the Security System Designer at time of final design documentation, and be re-confirmed by the Security System Contractor at the time of Security System bench testing.
   2) Shall be as approved and supported by DOC HQ IT
   3) For desktop PC's: Microsoft Windows XP
   4) For servers: Microsoft Windows Server 2008R2 (32-bit or 64-bit)
   5) Submit to DOC HQ IT a "Request for Approval of Non-Standard IT Equipment" for any devices that do not comply with the above requirements.

b. Service Packs and Patches
   1) Shall be the most current tested versions as of the time of Security System bench testing.
      a) For Microsoft Windows XP: Service Pack 3
      b) For Microsoft Windows Server 2008R2: Service Pack 1

2. Virtualization Software

a. Product and Versions
   1) VMWare – V-Sphere

3. Hardware

a. PC Workstation
   1) Manufacturer: Dell
   2) Processor: Intel Core 2 Quad 3.0GHz
   3) Memory: 4GB DDR3 SDRAM
   4) Video Card: 1GB minimum
   5) Supported Resolution: 1920x1200 minimum
   6) Removable Media Device (if Required): Min. 8x DVD-R
   7) Network: 10/100/1000BaseT Integrated Ethernet NIC
   8) Provide with Keyboard and Optical Mouse

b. Server
   1) Manufacturer: IBM
   2) Processor: TBD
   3) Memory: 4GB Minimum (size per software requirements)
   4) Video Card: Integrated for local administration
   5) Supported Resolution: 1280x1024 minimum
   6) Removable Media Device: Only as required
   7) RAID: Required - Hardware or software – Level TBD by Security System Designer (RAID-0 and RAID-1 are not acceptable)
   8) Network: Minimum (2) 100/1000BaseT Ethernet NIC
   9) Power Supply: Minimum (2) Redundant sized per hardware requirements

c. Desktop Monitor
   1) Minimum 22"
   2) Native digital display with DVI or HDMI
   3) Format: 16:9
   4) Touch-screen where required

4. Virus Protection
   a. Per DOC and ISB policies – Required for all servers
   b. Current DOC Standard: McAfee
5. Standards
   a. Comply with DOC Policies 280.100; 280.250; 280.300; 280.310; 280.825; 280.925; 400.030; 420.450; 700.130
   b. Comply with ISB Policies 400-P1; 401-S1; 402-G1; 500-P1; 501-S1; 502-G1; 700-P1; 701-S1; 702-S1; 704-S1; 1003.2-S; 1104.0-S
   c. WSDOC Telecommunications Distribution Infrastructure Standards Rev 5.3 (TDIS)

B. System "Time" Synchronization

1. NTP Service
   a. Shall reside on a non-virtualized server within the local area network
   b. Shall provide a single centralized time source for all security electronics servers and applications
   c. Shall provide Coordinated Universal Time (UTC).
   d. Individual hardware and software shall be configured for Pacific Standard Time Zone, with Daylight Savings Time adjustment.
      1) For Unix: Implement as a Daemon running continuously in user space (ntpd) with clock phase-locked loop in kernel space.
      2) For Windows: Implement Windows Time Service
   e. Applications shall be configured to use as authoritative time source
   f. Version: RFC 1305, NTPv3 or later
   g. All security systems shall reference as the authoritative time source to provide coordination of time across multiple platforms and systems.

C. Power Systems and Grounding

1. Surge Protection
   a. Provide surge protection devices (SPD's) on the panel(s) serving 208 or 120 VAC power to the Security System. Provide surge protection on both the input and the output of any UPS providing power to the Security System equipment. Rate the SPD per good engineering design.
   b. Provide building entrance protectors (BEP) on any new copper communications cable that exits/enters the building envelope. Provide protectors on each end of the cable. Protectors for any copper telecommunications cabling falling within 22-26 AWG shall be products conforming to the WSDOC TDIS.
2. Uninterruptible Power Supply (UPS) Systems
   a. System Performance
      1) Provide continuous power for all Security System components and the door locking devices, to include:
         a) All electromagnetic locks, solenoid or motor operated locks,
         b) All electrically powered sliding doors,
         c) The Access Control system and its components,
         d) The perimeter intrusion detection system,
         e) The Security Video System,
         f) The Security Audio Systems,
         g) All other devices controlled or monitored by the Security System.
      2) Each Security Electronic Equipment Room may be powered from a separate UPS.
      3) Minimum runtime shall be sixty (60) minutes under full load.

4) Maximum worst case designed load to be no more than 80% of rated capacity.
5) Units under 8kVA may be single phase 120/240 volt; Units 8 kVA or larger shall be three-phase 208Y/120 volt.
6) Output waveform distortion less than 5% total harmonic distortion.
7) Common mode noise rejection 120dB minimum.
8) Provide alarm contacts for trouble and inverter on.
9) Provide units capable of being assigned an IP address on the Security System network for monitoring of status and condition.

b. Acceptable Technology
   1) Double conversion, online, or other technology that provides no power break to the load on transfer to external power and back to UPS battery power.
   2) UPS shall utilize sealed batteries.

c. Installation
   1) Provide with external bypass and isolation switch sized for full load of connected UPS.
   2) Security System Designer should verify UPS location environment is adequate for heat removal and generated gas exhausting.

d. Performance Testing
   1) Verify bump-less transfer to UPS and return to external power.
   2) Load test to confirm run duration at full rated load.

e. Acceptable Manufacturers (all systems furnished under the project to be manufactured by same vendor)
   1) APC Technology
   2) Eaton "Powerware"
   3) Owner approved equal

3. Grounding

a. Provide a grounding bar in each Security Electronics Equipment Room equal to that specified in the WSDOC TDIS Grounding & Bonding specification. Main Security Electronics Equipment Rooms shall have a TMGB, and satellite rooms shall have a TGB. Provide grounding conductors sized per the WSDOC TDIS.

b. All equipment racks shall be connected to the main building ground at only one point in each building. All other grounds, such as chassis, shielded audio pairs, coax, bulkhead connectors, etc., shall be insulated from duct work, plumbing, or conduits, which in turn may cause accidental contact to the main station electrical ground at points other than intended.

c. The Security System Contractor shall ensure that all ground connections are in accordance with applicable codes and the WSDOC TDIS grounding and bonding specification.

d. Provide separate ground leads for equipment in control booths, control rooms, and control workstations.

e. Isolation transformers shall be provided as required to prevent ground loops from one power source to another.

f. Provide a green #12 grounding conductor in conduit to every new door frame having a lock or motor operator running at 120 volts or greater.

g. Provide grounding per NEC & WSDOC TDIS requirements.

D. Wire and Cabling

1. General Requirements

a. Conduit
   1) Minimum trade size shall be one (1) inch.

2) All security electronics wiring and cabling outside of Security Electronics Equipment Rooms shall be in metallic conduit or a metallic raceway.
3) PVC shall be allowed only when embedded in concrete walls with a minimum cover of two (2) inches of concrete, or where run a minimum of two (2) inches below the bottom of a slab-on-grade. Run no horizontal conduit within the slab-on-grade concrete.

b. Wireways are permissible in Security Electronics Equipment Rooms.
c. Wiring and Cables
1) Provide for separation of signal types. Install in separate raceways:
a) Power and Lighting (NEC Class 1)
b) Signaling (NEC Class 1)
c) Signaling (NEC Class 2/3)
d) Radio Frequency (video, television, and radio)
e) Low-Level Audio (Microphones) - Metallic raceways only, no PVC
f) Mid-Level Audio ("line level") - Metallic raceways only, no PVC
g) High-Level Audio (loudspeakers)
2) Provide wire and cable types per manufacturer's recommendations.
3) For all conductors entering or leaving a building envelope provide surge suppression appropriate for the signal type and level
4) All cables run below slab-on-grade or exterior to the building envelope shall be rated for direct burial or direct contact with water. Provide "Aquaseal" or equal direct burial rated cables in all locations where the conduit may fill with water.
d. Performance Testing
1) Achieve 100% successful testing of all wires and cables.
2) Test each conductor for continuity and ground.

E. Perimeter Intrusion Detection System

1. Basic System Description

a. Functionality
1) Provides detection for entire facility perimeter, without gaps, organized into zones.
2) Detects attempts to escape and/or movement in the perimeter penetration (sallyport) areas when such zones are active.
3) Provides detection for the perimeter edges of the rooftops of any building that intersects or penetrates the perimeter. Detects attempts to access the rooftop of such buildings from interior and exterior ways.
4) System control is by a touchscreen Alarm and System Management PC located in the Master Control Room (MCR) which has access to a Security System network printer for report output.
5) Provides system alarm and status annunciation to the Security System on all MCR control point workstations via dry contact relay output through the PLC. Zones in-alarm will only be available at the printer system touch screen.
6) Security Video System camera association with perimeter alarms is via dry contact relay output through the PLC.
7) Utilizes taut wire technology on the interior face of the inner perimeter chain-link fence, with detection extending 12" above the chain-link fence fabric.
8) Utilizes microwave protection (stacked dual zone) at vehicle sallyport and pedestrian sallyport openings in the perimeter.
9) System installation shall meet all applicable requirements of WSDOC TDIS.

2. Taut Wire Intrusion Detection System
   a. System Performance
      1) Is a zoned, supervised, detection system with continuously monitored sensor outputs.
      2) Provides very high probability of detection (POD).
      3) Provides very low false alarm rate (FAR).
      4) Provides very low nuisance alarm rate (NAR).
   b. Acceptable Technology
      1) Post sensors shall be a strain gauge (electromechanical transducer) type
      2) Field reporting units and processors will be located in enclosures located between the perimeter fence lines
      3) Local diagnostics and sensitivity adjustment of individual sensors in the field is via a laptop computer
      4) Diagnostics and sensitivity adjustment of individual sensors is from the Alarm and System Management PC
      5) Reports Alarm, Tamper, and Trouble conditions on the Perimeter Reporting Network
      6) Reports zone Alarms as left or right, corresponding to detection to the left and right of the sensor post.
      7) Reports alarms even if one or more sensors malfunction
      8) Continuously compensates for electrical and mechanical changes due to environmental effects
      9) Is of modular construction, designed for on-site repair by module/component replacement.
   c. Installation Standards
      1) The manufacturer should perform all aspects of the taut wire fence installation. The manufacturer shall have installed at least three (3) taut wire systems within the two (2) years immediately preceding the bid date of the project.
      2) Provide the complete inner perimeter fence system, excluding gates and gate operators, but with the foundations, rat wall or horizontal anti-dig provisions, fence posts, fabric, taut wire detection system, and related accessories under a single point of responsibility. Coordinate the installation with other site fencing for proper interface.
      3) Chain-link fence posts and foundations shall be engineered to accommodate all forces applied by the taut wire system, wind, and other required loads. Engineering shall be site-specific, based on local soil and environmental conditions, with engineering performed by a Structural Engineer licensed in the State of Washington; submit calculations for Owner review.
      4) Fence shall have either a 12” wide by 36” deep vertical rat wall directly under the taut wire detection, or, a minimum 4” thick by 72” wide concrete slab-on-grade extending under the taut wire detection as an anti-dig barrier.
      5) The bottom of the chain-link fence fabric shall have a bottom rail, set no more than 2” clear above the concrete, and which is secured to the concrete with an embedded steel strap at no more than 48” o.c.
      6) Fence fabric shall be 12’ high, 9-gauge galvanized, installed on the opposite side of the posts from the taut wire. All fence components shall be galvanized.
      7) All detection zones will be straight segments.
      8) Zones shall not exceed 300 feet in length.
      9) Install taut wire on the inside of the inner perimeter fence to provide detection from grade to 12 inches above the fence fabric. Standoff the taut wire sensor channels and anchor channels from the support posts.
      10) Taut wire strands shall be double-braided with a reverse twist, high tensile strength wire with external barbs, Bezinal® (95% Zinc + 5% Aluminum corrosion resistant) coated wire 15.5 AWG.

11) Support taut wires with slider posts and extenders. In corrosive environments consider using stainless steel anchor posts and stainless steel tensioners.
12) Bottom strands to start no higher than 4 inches above rat wall or slab-on-grade, then
    a) Space strands at 4 inches to a height of 48 inches above ground
    b) Space strands at 5 inches for the next 60 inches above ground
    c) Space remaining strands at 6 inches.
    d) Total strand count = 32.
13) Furnish programming and diagnostic kit, including licensed software, for maintenance use. (Provision of a laptop computer for field maintenance is not required.)
14) Provide full training for owner's maintenance staff, and separately for custody officers.
15) Furnish manufacturer's recommended spare maintenance parts, but no less than one (1) processor circuit board, one (1) transponder, sixty-four (64) sensors, sixty-four (64) breakaway tab anchors,1,320' of Bezinal® double-braided wire, and four (4) tensioners.

d. Performance Testing
    1) Deflection force for alarm actuation shall not be less than 20, or more than 50 pounds.
    2) Deflection shall not exceed three and one half inches (3-1/2") without actuating an alarm.
    3) Test each strand at two (2) locations in each zone fifteen (15) feet from the zone's end anchor posts.
    4) Annunciation of each actuation shall be signaled on the Perimeter Reporting Network and be confirmed at all annunciation devices.
    5) Testing to be witnessed by Owner's representative(s) as designated.
e. Acceptable Products and Manufacturers
    1) Provide a taut wire perimeter intrusion detection system that is installed and operating at three (3) locations in the United States having perimeters of at least 3,000' each.
    2) The following manufacturers are pre-approved:
        a) DeTekion Security Systems, Inc
        b) Senstar (DTR-3000)
        c) As owner approved

3. Microwave Detection System

a. System Performance
    1) Detect motion from ground surface to +8 feet elevation within the effective zone area.
b. Acceptable Technology
    1) FCC certified X-band
    2) Adjustable sensitivity
    3) Selectable channels
c. Installation Standards
    1) Dual stacked sensors at inner boundary of all sallyports penetrating perimeter
    2) Microwave zones to crossover or overlap taut wire zones without gaps in perimeter detection
    3) Ground surface to be level and uniform throughout detection zone, and without standing water or other features which might affect detection
    4) Local identification and adjustment of individual sensors
    5) Report Alarm, Tamper, and Trouble conditions to the Perimeter Reporting Network
d. Performance Testing
    1) Fast and slow walk through zone - 100% detection
    2) Fast and slow crawl through zone - 100% detection
    3) Tests to be performed at both ends and the center of each zone
    4) Annunciation of each actuation shall be signaled on the Perimeter Reporting Network and be confirmed at all annunciation devices.

e. Acceptable Manufacturers
   1) Southwest Microwave
   2) Senstar
   3) As Owner approved

4. Rooftop Outdoor Microwave Transceiver System
   a. System Performance
      1) Target minimum cross section .07 square meter will be detected when moving at 0.2 to 26 ft/sec.
      2) Coverage pattern – for prone crawling 150 ft long by 15 ft wide.
      3) Coverage pattern – for person walking 200 feet long by 24 feet wide.
      4) Range cutoff adjustment adjustable from 50 feet to 200 feet.
      5) Synchronization shall be provided for multiplexing units together to eliminate mutual interference.
   b. Acceptable Technology
      1) K-band microwave intrusion sensor with range cutoff capability
      2) Independent pattern length and width adjustments
   c. Installation Standards
      1) Housing shall be outdoor rated -30F to +150F
      2) Meet all FCC rules & regulations
      3) Provide rigid mounting meeting requirements of manufacturer.
      4) Adjust pattern and mounting angles to optimize coverage.
      5) Provide certification from the manufacturer that the installation meets all their requirements and is fully warranted.
   d. Performance Testing
      1) Perform walk and crawl tests as described in manufacturer's instructions.
      2) 100% field functional test, witnessed by owner's designated representative(s)
      3) Annunciation of each actuation shall be signaled on the Perimeter Reporting Network and be confirmed at all annunciation devices.
   e. Acceptable Manufacturers
      1) Southwest Microwave Model 380
      2) As Owner approved

5. Perimeter Reporting Network
   a. System Performance
      1) Multiplex alarms and other conditions to a central processing location
      2) Receive input from Taut Wire Processors, and Microwave Links
      3) Central processor will interface with the Security System by outputs to the PLC for annunciation of system status and alarm conditions by zone and type on Master Control Room control panel touchscreens.
      4) System management and alarm control is on the Alarm and System Management PC
   b. Acceptable Technology
      1) Multiplexed controller with an RS-422 network communications loop
   c. Installation Standards
      1) All CPU equipment shall be installed in Security Electronics Equipment Rooms. Provide KVM extensions to the Main Control Room for system status, alarm annunciation, and system control
      2) Central control unit located in Security Electronics room.
      3) Cabling per manufacturer requirements
      4) Comply with WSDOC TDIS as applicable.

d. Performance Testing
   1) Tested during testing of Taut Wire and Microwave systems
   2) Verify each enclosure tamper alarm
   3) Annunciation of each actuation shall be confirmed at all annunciation devices.

6. Perimeter Security Enclosures

   a. System Performance
      1) Enclosure for field located sensor controllers, processors and transponders for the Taut Wire, and Microwave sub-systems.
      2) Also may contains interfaces for perimeter CCTV camera to fiber adapters
      3) Power conversion from UPS power distributed from the Security Electronics room to voltages required by the various components installed or connected
      4) Provide tamper switch on door
      5) Provide with keyed-alike locks
   b. Acceptable Technology
      1) NEMA 4 – non-corrosive fiberglass or stainless steel enclosures are preferred
      2) Sized as needed for equipment
      3) Provide screened ventilation and/or heaters as required to maintain proper environmental conditions for the installed equipment, as required for the site's climatic conditions.
   c. Installation Standards
      1) Ground to common fence grounding ring
      2) Interconnect enclosures with 2-inch minimum size underground conduits
      3) Provide one (1) spare 2-inch conduit for future system needs or changes
      4) Comply with WSDOC TDIS as applicable
   d. Performance Testing
      1) Tested during installed systems testing
   e. Acceptable Manufacturers
      1) Hoffman
      2) As owner approved.

F. Door / Gate Control and Monitoring Systems

1. Definitions

   a. Door – For purposes of this section, any swing or sliding door or frame fitted with an electrically operated locking mechanism and/or a position sensor, intended for connection to a control circuit.
   b. Gate – For purposes of this section, any interior or exterior swing or sliding gate that is fitted with an electrically powered operator, an electrically operated locking mechanism and/or a position sensor intended for connection to a control circuit.
   c. Door/Gate Control System – Any system intended to limit access to or egress from a specified area separated with a door or gate.
   d. Monitoring System – Any system intended to report unauthorized entry/egress into/out of an area separated by a door or gate.

2. System Description

   a. A complete Control and Monitoring system consists of a data network to interconnect the various system nodes (PLCs), and an HMI device for interfacing the technology to the operator and the control/monitoring logic. This section addresses only the control/monitoring logic. The data network and the HMI are addressed in other sections of these Guidelines.
   b. Door/Gate Control – This system provides remote operational control for doors/gates associated with penetrations through security lines or separations, both inside buildings and on the facility site. This system consists of an operator interface (HMI) to permit control by the operator, hardware

and/or software in a custom arrangement to effect the control and feedback required to implement the Operational Narrative for the system, and the interconnections with associated locking, sensing, and/or communication systems. Control systems should always be designed to "fail secure." To the greatest extent possible, any power failure, wire break, short circuit, or component failure will move the system to a more secure condition, and annunciate/report the problem.

c. Door/Gate Monitoring - This system is intended to provide continuous monitoring of a specific area from a remote location. This monitoring may be implemented through sensors associated with electrical or mechanical door/gate locking mechanisms, or through separate sensors utilizing other technologies. In all cases, implementation of the Operational Narrative for the system must be provided. Monitoring systems are always designed to "report a failure." To the greatest extent possible, any power failure, wire break, short circuit, or component failure, will annunciate/report the problem.

3. Technology

a. The preferred technology for implementation of the Door/Gate Control and Monitoring System is through the use of one or more Programmable Logic Controllers (PLC's). Once a manufacturer is established for a system, use only the accessory components specifically recommended by the manufacturer for use with that equipment. Do not use generic input/output, power supplies, etc.

b. For existing facilities with other PLC equipment installed, use the same manufacturer as the existing systems. For new facilities or existing facilities with no PLC equipment, the preferred equipment should be the products of one of the following manufacturers that conform to requirements of these Guidelines:
   1) Square D Modicon
   2) Allen Bradley
   3) General Electric
   4) Or as Owner approved

c. Software and firmware used in conjunction with the PLC equipment should become the property of WSDOC following project acceptance, and should be the most recent version available on the date of the bench test.
   1) Software provided should include the programming application used in development of the PLC programs installed and copies of the most recent programs. Provide any special cables needed to allow programming to be loaded into the system from an Owner-provided standard laptop PC at a system PLC port
   2) Programming should use plain English or standard ladder logic, and should have sufficient commenting to facilitate debugging and modifications

d. To the maximum extent possible, Control and Monitoring systems should be designed without a single point of failure. When more than one (1) PLC resides on a network, each PLC should be configured to take over control from any failed PLC, remove the failed PLC from the network, and report the failure to the associated HMI(s) and/or workstation(s) .

e. When the system includes a single PLC with more than 120 controlled or monitored doors and gates, or when the system includes more than one PLC with a total of more than 250 controlled or monitored doors and gates, provide a cold, shelf-stand-by PLC with all accessories, that can be used for quick replacement of a failed PLC.

f. These systems should be designed specifically to be fully operable using local peer-to-peer network configurations. Workstation PC's utilized as a part of the control and monitoring system should operate in a peer-to-peer manner, and should not be dependent upon a server for basic functionality in the designated control and monitoring area. Servers associated with control and monitoring systems should be dedicated as servers.

g. Door/gate sensors for use with these systems include IR, microwave/Doppler, photoelectric beam, magnetic, capacitive, proximity, and other detection methods. In some cases, sensors can be

combined or interconnected to assure the desired information is being monitored. (For example, to assure a door is both closed and locked the 'door position switch' and the 'lock bolt switch' may be wired in series.) Monitoring is frequently dependent upon time of day, or must be bypassed for authorized access without alarming. Hence, where required, a bypass function with a warning indicator may be required in the HMI.

4. Installation
   a. All control and monitoring equipment should be installed in a secured Security Electronics Equipment Room, and is to be grounded in accordance with requirements found elsewhere in these Guidelines.
   b. All control and monitoring equipment should be provided operating power from a UPS and generator backed source.
   c. All control and monitoring equipment should be designed with or provided with dual regulated power supplies arranged to automatically switch to the backup if/when the primary supply fails. At the same time, the operator should be advised of the failure.
   d. All circuits entering or leaving the Security Electronics Equipment Room (input and output, power and signal) should be provided with individual fuses to protect the system equipment against cascading failures due to a single event.
   e. All low voltage power, signal and control circuits should be wired only in metallic raceways, with insulated, color coded wires. Underground/under slab PVC conduit for signal level circuits and ground return circuit configurations will be rejected.
   f. Spare conductors should be provided in each cable run to facilitate maintenance and future system modifications.
   g. The same conductor colors should be used for similar circuits within the project. The preferred color coding scheme should be as follows:

1)	Black	Primary lock voltage
2)	Red	Lock
3)	White	Primary lock voltage neutral
4)	Green	Ground
5)	Brown	Secure
6)	Blue	Unsecure
7)	Orange	Offender control
8)	Yellow	Unlock
9)	Purple	Spares
10)	Gray	Spares
11)	Pink	Spares
12)	Tan	Spares

5. Operations
   a. Control and monitoring systems, implemented with the use of any technology, should perform in accordance with pre-defined Operational Narratives developed by the Security System Designer. These narratives should be a part of the project design documents and should provide a step-by-step functional and sequential description of each required control sequence. Each narrative should consist of two (2) parts: 1) a true pictorial depiction of the control element as it will appear on the HMI for the control operator; and 2) a written step-by-step description of the sequence of operation. Each Operational Narrative should be edited for specific application to the project for which the documents are intended. Generic narratives or sequences of operation will be rejected.
   b. An example Operational Narrative written for use with a 'touchscreen' HMI can be found at Section VIII of these Guidelines.

c. Operational Narratives will likely be used more than once for a project. The documents should clearly identify each instance that the system Operational Narrative is applied with a unique identifier which should be referenced consistently in the drawings and/or specifications. The identifier should enable easy identification of the door/gate or room number and its Operational Narrative.
d. Control systems should have a maximum operation and feedback response time limit of 250 milliseconds. This means that following a manual control input at the HMI, the following should occur within 250 milliseconds (plus the operational time for sliding doors/gates or motorized locking mechanisms):
    1) The system should recognize and report receipt of the command (visually and/or audibly).
    2) The system should verify the logic associated with the command, and if permitted by the logic, should transmit a signal for the action desired.
    3) The action should be recognized by the system as a status change.
    4) The status change should be reported on the HMI.
e. Monitoring systems not associated with a controlled event should have a maximum reporting time of 500 milliseconds. Indications should be returned from sensors when a status change occurs. Monitoring systems that are part of a control system should conform to the requirement for control systems.

6. Performance Testing
    a. Demonstrate proper operation and response time for each instance of each Operational Narrative at each control workstation.
    b. Simulate utility power failure and demonstrate continuance of proper operations under failure of normal power conditions – with and without the UPS being supplied from the generator. Also demonstrate a return to normal power supplying the UPS.
    c. Simulate failure of each primary power supply and demonstrate automatic switchover to the backup power supply and the notification to the operator. Also demonstrate a return to the primary power supply when it is restored.
    d. Demonstrate a maximum enclosure ground resistance at each equipment room/area of 10 ohms or less from the equipment enclosures to the building ground point.
    e. Coordinate with the detention equipment and the gate suppliers/installers to assure proper physical operation of the gates and setting of the required limit switches and other sensors associated with the doors and gates.

G. Security Video System

1. Definitions
    a. Video camera – A commercially available, color, low light level, high resolution, progressive scan, CCD image sensor fitted with an appropriate fixed or variable focal length lens and arranged for "Power over Ethernet" (POE) where available, or provided with a power supply. May be pan-tilt-zoom type.
    b. Network Video Recorder (NVR) – A distributed and networked system that records digital video data from video cameras, transmitted over a data network.
    c. Digital Video Recorder (DVR) – A self-contained device that records digital video images from analog video cameras.
    d. Hybrid Video Recorder (HVR) – A self-contained device that records digital video images from analog or digital video cameras.
2. System Description
    a. A Network Video Recording system consists of video cameras, video servers, computer workstations, managed network switches, network video recorders, and network video

management system (NVMS) software. Video cameras, computers workstations, network video recorders and network video management software are discussed in this section.

b. Extensions to existing NVR systems should match the characteristics, performance and features of the existing system. (Particular attention to system software version(s) and availability of new licenses is cautioned.)
c. New NVR systems should provide recording and video coverage of the specified areas, and should integrate with control systems to provide live images and "call up" capability for any camera in the system in a manner that is transparent to the operator. System may be searched and authenticated copies made without affecting realtime system operations. NVR systems should be provided with capacity, without NVMS upgrading, for double (2x) the number of installed cameras, and with licenses for 110% of the number of installed cameras.
d. In addition to recording and storing video images, NVR systems should display 'live', high resolution color video images on demand at any or all authorized workstations on the network. Available images at a given workstation may be restricted to local cameras, and access to archived video may similarly restricted. Individual workstations may select a preferred display format including single image, 4 images, 9 images or 16 images simultaneously. In addition, images should be available for "call up" by other associated systems via digital signal or relay contact.
e. A DVR or an HVR system should be specified only as an extension to an existing DVR system, or for a small system achieving the required coverage with 16 or fewer cameras and confined to a limited area of the facility, and having only one (1) or two (2) monitoring workstations. Extensions to these existing systems should include either analog or digital cameras to match the existing, but it is preferred that new systems employ digital IP cameras. At least 20% of the available analog ports should be left unused for future expansion. Provide licenses for 110% of the number of installed cameras. A DVR or HVR system may be searched and authenticated copies made without affecting realtime system operations.
f. Video coverage should be as specifically determined for each project. Fixed focal length cameras, or cameras having a variable focal length lens which is adjusted at time of installation, are preferred, but some circumstances will require Pan-Tilt-Zoom arrangements. PTZ cameras should be controlled by a physical "joy stick" and should be programmable to pan and zoom to at least 12 preset fixed aim points at the press of a physical or virtual button, or closure of a form 'C' remote contact.

3. Technology

a. Digital IP color video cameras should meet the technical requirements described below and should include an integrated encoder providing a TCP/IP format output via a compatible RJ-45 Ethernet jack.
b. Analog color video cameras should provide a 1v peak to peak composite video output signal at the camera into a 75 ohm load with the imager illumination described below.
c. All video cameras should support motion sensing and analysis based on pixel change in a region of the image that is selectable as to size and location within the total image.
d. Cameras should employ automatic coverage control to switch from bright scene color image to dark scene monochrome image.
e. Megapixel IP cameras may be appropriate for some applications.
f. Power over Ethernet (PoE) should be utilized as the preferred camera power source whenever possible.
g. All video cameras should meet or exceed the following specifications:
    1) Bright Scene Color Sensitivity – full video @ 0.3fc; useable picture @ 0.07fc
    2) Dark Scene Monochrome Sensitivity – full video @ 0.12fc; useable picture @ 0.03fc
    3) Automatic changeover from Bright to Dark Scene operation & reverse
    4) Automatic white balance at 3200K indoors and 5500K outdoors

5) Backlight compensation
6) Dynamic range – 60dB
7) Signal to Noise Ratio – 50 dB
8) Synchronization – internal line lock
9) Vertical phase delay adjustment – 0 – 360 degrees
10) Shutter – Automatic ranging 1/50 to 1/5000 second
11) Withstand direct or reflected sunlight without detrimental effects
12) Video compression – H.264; M-JPEG; JPEG
13) Sensor Resolution – 4 CIF (704 x 576 h/v)
14) Frame Rate – H.264 @ 1 to 60; M-JPEG @ 1 to 30 for 4 CIF

h. New NVR systems should record all connected video cameras in one more of the following selectable and time-programmable modes:
   1) Continuously at 30 frames per second at 4CIF
   2) Continuously at 10 frames per second at 4CIF
   3) Continuously at 3-5 frames per second, except when motion is detected go back 10 seconds in time and record at 30 frames per second at 4 CIF until 5 minutes after the motion stops, then return to 3-5 frames per second.
   4) Record at preset frame rates during preset time periods.
i. Both DVR and NVR systems should have online storage capacity in a RAID 5 or RAID 6 configuration equivalent to at least 1.2 times the number of installed video cameras recording continuously at the highest resolution, 10 frames per second, for 30 days. System should overwrite stored data after 30 days in a "first in – first out" type housekeeping.
j. DVR storage systems should be provided in a configuration that allows for expansion of the online storage through the installation of additional hard drives only.
k. NVR systems should be designed for resiliency and failure tolerance, through failover or virtualization strategies.
l. NVR storage systems should implement a dedicated iSCSI Storage Area Network (SAN) architecture. NVR storage systems should utilize RAID 5 or RAID 6 as a storage requirement. All storage systems should be of a scalable type to allow future increases in storage requirements.
m. DVR, HVR, and NVR systems should continuously stamp the recorded data with date and time, and store the information in computer memory. The system should continue to monitor in real time, present live images in real time, and record in real time, while being searched by date and time, all simultaneously at one or more authorized and password protected workstations. Copies of selected segments with authentication (for evidence purposes) may be made and transferred to portable media at designated workstations only. System shall have a track record of providing authenticated video accepted in courts of law.
n. Images or system functions in use at one location or workstation should not affect any function or operation at any other location or workstation. Pan-Tilt-Zoom control may be prioritized by workstation. The Search and Copy process should not affect any other feature or operation of the system.
o. Where applicable, video equipment should conform to the most recent ONVIF version 2 interoperability specification.
p. Video systems should use a single manufacturer's products wherever reasonably possible. Use accessory components specifically recommended and supported by the manufacturer for use with that equipment. All video components should be verified compatible with each other. Do not use generic I/O, power supplies, etc. For existing facilities with other video equipment installed, use the same manufacturer as the existing systems. For new facilities, or existing facilities with no video equipment, the preferred equipment should be products of the following manufacturers that conform to the requirements of these Guidelines:

1) Cameras:
   a) Bosch
   b) Vicon
   c) Owner Approved
2) NVMS Software:
   a) Genetec
   b) OnSSI
   c) Owner Approved
3) Encoders:
   a) Bosch
   b) Vicon
   c) Owner Approved

q. Software and firmware used in conjunction with the video equipment should become the property of the State following project acceptance and should be the most recent version available on the date of the bench test. Software should include a programming application to allow changes/adjustments to the program using plain English or ladder logic via an off-line PC which can then be loaded into the system at any NVR port.

r. The Network Video Management System (NVMS) should be a proven application that
   1) Is server based, running the latest version of the software available on the date of the bench test
   2) Requires only a standard computer server without special hardware or software (other than the NVMS software)
   3) Should accommodate an Ethernet based network and utilize TCP/IP communication protocol.

s. The NVMS should
   1) Incorporate distributed architecture for full redundant recording
   2) Provide full automatic failover protection and return as a basic feature
   3) Support analog video (NTSC at 1v p-p) via multiple encoders.
   4) Allow a different format selection for each camera individually using common video compression formats including H.264, JPEG, M-JPEG, MPEG2, MPEG4
   5) Provide full operation using CIF, 2CIF, VGA, 4CIF and Megapixel resolution
   6) Allow live monitoring and recording simultaneously
   7) Allow search and copy operations without affecting the live monitoring and recording functions

4. Installation

a. All video equipment (except cameras) should be installed in a secured Security Electronics Equipment Room, and be grounded in accordance with requirements found elsewhere in these Guidelines.

b. All components of the Security Video System should be provided operating power from a UPS and generator backed source.

c. Camera locations and their views should be approved by the Owner. As a pre-condition to installation the installer should demonstrate available images using a live camera provided with a manual vari-focal lens and a color display. Handhold the camera at the proposed installation location and demonstrate available images by changing focal length of the vari-focal lens until an acceptable image is identified by the Owner.

d. Cameras intended to provide images with identifiable subjects (“head shots”) should be provided with a lens to produce an image that presents the subject’s face as not less than 1/3 the total height of the image on the screen.

e. Cameras mounted outdoors, or indoors where the field of view is influenced by changes in ambient lighting, should be provided with an auto-iris lens. Some design conditions may warrant provision of a camera having capabilities for overcoming strong backlighting.

f. Cameras should be rated by the manufacturer for installation under the environmental conditions expected at the installation location. Cameras may be provided with a heated and/or cooled environmental enclosure that will limit and/or control the camera environment to within the manufacturer's rating. In addition, security enclosures should be provided for cameras installed in offender accessible locations if less than twelve feet (12') above the highest access level within ten feet (10') of the camera. Enclosure/camera selections should assure the enclosure does not limit the camera view.
g. Not more than 75 percent (75%) of the number of video cameras recommended by the manufacturer as the maximum number of cameras supported by a video server should be connected to a server.
h. Systems with more cameras should use multiple video servers, which may be distributed throughout the facility, connected on a dedicated video network with managed virtual switching.
i. Failure of one video server should cause video images after the failure to be recorded at a different video server for the duration of the failure without operator or technician intervention (automated failover), and report the failure to the Security System Management PC.

5. Operations
   a. Video systems provide assistance to correctional staff in at least the following ways:
      1) Extension of the area that can be visually observed
      2) Provide positive visual identification before opening doors/gates
      3) Record video at time dependent, selectable rates
      4) Detect, Report and Record activity (motion) in areas under video surveillance, at time dependent, selectable rates
      5) Store video images for a pre-defined period
      6) Search the stored data and produce portable authenticated evidence copies of events
   b. Video systems provide all of the following image types simultaneously at any or all authorized workstations on the system:
      1) Dedicated Images - Images always on screen for observation
      2) 'Call Up' Images - Images displayed only when a related system triggers the need for a video picture (verification of persons desiring passage into or out of a facility)
      3) 'On Demand' Images – Images not displayed until specifically requested by a person having authorized access to the system
   c. The video system should respond to commands and display the full resolution and full quality image requested within 100 milliseconds of a call transmitted by digital message or contact closure. The image should not roll or tear, or display any degrading characteristics (snow, sound bars, etc) at any time, but should remain stable without a change in resolution or quality until cancelled by another digital message or contact closure, or through expiration of a timed operation.

6. Performance Testing
   a. Demonstrate proper operation and quality images for all cameras and workstations. Images displaying sound bars or that roll or tear, or display degrading characteristics will be rejected.
   b. Demonstrate acceptable response time for 25% of each image type described above in the Operations section.
   c. Simulate utility power failure and demonstrate continuance of proper operations under failure of normal power conditions - with the UPS being supplied from the generator. Also demonstrate a return to normal power supplying the UPS.
   d. Simulate failure of each primary power supply and demonstrate automatic switch over to the backup power supply with notification to the operator. Also demonstrate a return to the primary power supply when it is restored.

e. Demonstrate a maximum enclosure ground resistance at each equipment room/area of 10 ohms or less from the equipment enclosures to the building ground point.

H. Intercom Systems

1. Definitions
   a. Intercom System – a system that provides audio communications between two or more locations. There are generally three types:
      1) Cell intercom
      2) Door/Gate intercom
      3) Visitor/Offender intercom
   b. Master intercom station – an intercom station located at a control workstation that selects the remote station to be contacted and controls the communication.
   c. Remote intercom station – an intercom station located at the non-control end of the communication. Usually includes a call button to request communication with the master intercom station.
   d. Intercom amplifier – a bi-directional amplifier designed specifically for intercom systems.
   e. Station Select button – a physical or virtual pushbutton that determines which remote intercom station will be connected for communication with the master intercom station.
   f. Push-To-Talk button – a physical or virtual pushbutton that controls the direction of the communication once it has been established.
   g. Visitor/Offender intercom stations - a pair of handsets or wall mounted speakers on opposite sides of a non-contact visit booth that provides a means of communication between one visitor and one offender.
2. System Description
   a. Cell intercom – consists of master and remote intercom stations and provides controlled communications between the control workstation and each offender cell
   b. Door/Gate intercom – consists of master and remote intercom stations and provides controlled communications between the control workstation and a door or gate
   c. Visitor/Offender intercom – consists of simple handsets or wall mounted speakers and provides unattended communications between a visitor and an offender in non-contact visiting areas
3. Technology
   a. An integrated digital audio system to provide intercom, paging, talk-back paging, telephone interface and other applications is preferred. These shall conform to the requirements of these Guidelines, and to the requirements of the TDIS.
   b. Analog based intercom systems should be of a type that will allow Ethernet interconnections between equipment head end locations.
   c. Amplifiers should be full duplex.
   d. Intercom speakers should be specifically selected for clarity and intelligibility of the human voice.
   e. Call buttons for remote intercom stations should be tamperproof, should include a positive stop when the button is depressed that is independent the electric switch, should provide a spring return when released, and should provide no means for disassembly from the operating side.
   f. Remote intercom stations should be heavy duty, tamperproof and provide no means for disassembly from the operating side.
4. Installation
   a. Provide an intercom amplifier for each master intercom station. Locate the amplifier in a designated secured electronic equipment room. Ground the system in accordance with requirements found elsewhere in these Guidelines.

b. All components of intercom systems should be provided operating power from a UPS and generator backed source.
c. Intercom stations should be wired separately from other systems in grounded metallic conduit. Station cables should be continuous from point to point, without splices. Route station cables away from sources of interference including:
    1) Lighting fixtures
    2) Heating/cooling/ventilating equipment
    3) Radio communication equipment
    4) Transformers
    5) Motors
d. Wall mounted intercom stations in areas accessible to offenders and below twelve feet (12') above the floor should be mounted in a flush enclosure with a protective security baffle that prevents insertion of objects that could damage the station.
e. Remote the intercom amplifier master volume control to make it accessible at the control workstation(s).

5. Operations
    a. Cell Intercom system provides communication between a control workstation and offender cells (and may be used for other selected locations requiring communication). Communication can be established with one or several cells simultaneously by selecting one or more Station Select buttons. Communication is controlled by the master intercom station with the Push-To-Talk button. With this button depressed, the master intercom station talks and the remote intercom station listens. With this button not depressed, the master intercom station listens (hands-free) to the remote intercom station. Control may also covertly monitor offender cells. (When employed for non-cell applications the sounding of a "connect" tone at the remote station may be required.) Cells may call the control master intercom station by pressing the call button which sounds a call tone and starts a call in signal flashing. Regardless of how many times the call button is pressed, the signal will sound only once until answered or reset by the control workstation.
    b. Door/Gate intercom system provides communication between a control workstation and a secured movement door or gate. Communication is established with the door/gate by selecting the Station Select button. Communication is controlled by the master intercom station with the Push-To-Talk button. With this button depressed, the master intercom station talks and the remote intercom station listens. With this button not depressed, the master intercom station listens (hands-free) to the remote intercom station. Control may also covertly monitor the vicinity of a door or gate. Remote intercom stations at doors or gates may call the control master intercom station by pressing the call button which sounds a call tone and starts a call in signal flashing. Regardless of how many times the call button is pressed, the signal will sound only once until reset or answered by the control workstation.
    c. Visitor/Offender intercom system - Once activated by the control operator, this system provides a half-duplex communication link if wall speakers are used or a full duplex link if handsets are used. The link between the two speakers or handsets is maintained without further attention by the control point. A timing system may break the communication link after a pre-set time to control the visiting period. Provide for an audio output means to interconnect an audio recording device at a future time.

6. Performance Testing
    a. Demonstrate proper operation and sound quality for all intercom stations at an 80 dB level. Audio with audible hum, sizzling, clicks, pops or other interference will be rejected. Sound level at each intercom station should be demonstrated at 80 dB measured 1 meter from the speaker.

b. Intercom audio should not transition from standby to full power and back to standby after each use but should remain always available.
c. Set initial levels after testing at nominally 15 dB above the ambient noise level when the facility is in normal operation.
d. Simulate utility power failure and demonstrate continuance of proper operations under UPS/generator power. Also demonstrate a return to utility power from UPS/generator power.
e. Demonstrate a maximum enclosure ground resistance at each equipment room/area of 10 ohms or less.
f. Demonstrate isolation between visitor/offender intercom station pairs of at least 55 dB.

I. Paging Systems

1. Definitions

a. Paging Access – the manner in which a page is originated. Some of the possibilities for originating a page message include: a handheld or desk microphone with push-to-talk button; a panel mounted, usually shared, speaker/microphone and push-to-talk button; integration with the facility intercom system; integration with the facility telephone system.
b. Talk-back Paging – a paging system that provides for a response from the paged area, ie: the ability for the paged area to "talk back" to the originator of the announcement or message.
c. Overhead Paging Speaker – A paging system speaker mounted in the ceiling, suspended from the ceiling or mounted on a wall or parapet. Preferably, the speakers selected are specially designed to:
    1) Improve intelligibility
    2) Enhance the frequencies associated with human voice
    3) Reduced echoes in acoustically 'hard' environments
d. Paging Amplifier – A remotely enabled audio amplifier to drive the overhead paging speakers and specially designed for frequencies associated with human voice.

2. System Description

a. Paging Systems are used to allow announcements, messages, etc to be initiated from one or more originating locations and heard and understood at one or more listening locations. Access to these Paging Systems is with the use of a shared, panel mounted or desk microphone or through an interface via the facility intercom system or administrative telephone system.
b. Talk-back paging is similar to a standard paging except that "talk-back" from the paged area is possible, under control of the initial paging location.

3. Technology

a. Paging amplifier should be solid state type providing specific multiple inputs for all required input sources (hi- and low-impedance microphones, auxiliary inputs and telephone paging interface. Each input should have its own level control in addition to a master volume control. Amplifiers should provide automatic level control, automatic muting (telephone input), microphone precedence, electronic overload protection and a ten frequency, 2/3 octave boost/attenuation equalizer/feedback filter. Amplifier specs should meet or exceed the following:
    1) Power Output: As required to meet SPL and rated distortion requirements.
    2) Frequency Response: 100 to 10KHz, +1 dB
    3) Distortion: 0.5% max
    4) Signal/Noise: -94 dB min
    5) Equalizer ISO freq.: 10 frequencies from 60 to 5KHz
    6) Output: 8 ohm, 25V, 70V
b. Analog based paging systems should be of a type that will allow Ethernet interconnections between equipment head end locations.

c. Paging speakers for indoor use should be distributed throughout the zone and should meet or exceed the following:
   1) Frequency Range: 100 to 05KHz, +8 dB
   2) Dispersion: 75 degree cone
   3) Power Capacity: 10W program
   4) Taps (25/70v line): 5 steps or more from 0.1 to 10 watts

d. Paging horns located outdoors should be rated for the environment and should meet the same minimum specifications as noted above except:
   1) Dispersion: 120 degrees (h) x 90 degrees (v)

e. Telephone paging interface provides a bridge between the telephone exchange and the paging amplifier and should meet or exceed the following:
   1) Port Access: Trunk or station port
   2) Ringer Equiv: 1.2B (2 wire analog)
   3) Frequency Range: 100 to 10KHz
   4) In/Out Impedance: 600 ohms

f. Talk-back paging amplifiers should be half-duplex intercom type allowing communication in both directions. Control of the talk-back paging amplifier should rest with the control workstation.

g. Some installations may select an integrated digital audio system to provide intercom, paging, talk-back paging, telephone interface and other applications. These are acceptable if conforming to the requirements of this Guide.

4. Installation

a. Provide a paging amplifier or talk-back paging amplifier for each paging zone. Locate the amplifier in a designated secured electronic equipment room/closet. Ground the system in accordance with requirements found elsewhere in this Guide.

b. All components of paging systems should be provided operating power from a UPS and generator backed source.

c. Wherever possible, provide more than one paging speaker in each zone. Paging speakers should be deployed in a manner that allows a uniform 15dB above the ambient noise level in all areas of the paging zone. Speakers should be wired separately from other systems in grounded metallic conduit. Speakers in the same zone should be wired to a dedicated zone cable extending back to the amplifier. Speaker cables should be continuous from point to point without splices. Route speaker cables away from sources of interference including:
   1) Lighting fixtures/ballasts
   2) Heating/cooling/ventilating equipment
   3) Radio communication equipment
   4) Transformers
   5) Motors

d. Wall mounted speakers in offender areas below twelve feet (12') above the floor should be mounted in a flush enclosure with a protective security baffle that prevents insertion of objects that could damage the speaker.

e. Speakers mounted outdoors should be 'aimed' to obtain the required coverage.

f. Use the amplifier input level controls and master volume control in addition to the multi-taps on the speaker matching transformers to balance and set the level for each paging zone. Adjust the equalizer settings for best sound intelligibility.

5. Operations

a. After zone selection at the control panel communication is amplified through the paging amplifier and broadcast to the paged space via the paging speakers. Alternately, zone selection is

automatic if each zone is provided a unique extension number on the administrative telephone system.

b. Talk-back paging operates as above, and in addition communication is controlled by the control panel with the Push-To-Talk button. With this button depressed, the control panel operator talks and the remote location(s) listen. With this button not depressed, the control panel operator listens to the remote location(s).

6. Performance Testing

a. Demonstrate proper operation and sound quality for all zones. Audio with audible hum, sizzling, clicks, pops or other interference will be rejected. Sound level throughout the zone should be demonstrated at 85 dB measured 1 meter from the speaker.
b. Paging audio should transition from standby to full power in less than 50 milliseconds without audible noise or interference.
c. Set initial levels after testing at nominally 15 dB above the ambient noise level of the facility in each installation location when in normal operating mode.
d. Simulate utility power failure and demonstrate continuance of proper operations under UPS/generator power. Also demonstrate a return to utility power from UPS/generator power.
e. Demonstrate a maximum enclosure ground resistance at each equipment room/area of 10 ohms or less.

J. Access Control System

1. Definitions

a. Access Control System - a system that grants access to restricted spaces only to authorized users.
b. Access Credential – encoded cards or other physical devices that can be read by a slide or a proximity reader. Types include: proximity, barcode, magnetic stripe, and RFID.
c. Reader – a compatible device to read the information on an Access Credential.
d. Keypad – a number pad with 10 or more buttons allowing input of coded numbers.
e. Biometric Reader – a reader designed to read a physical trait of users such as fingerprints, iris/retina, palm, etc.
f. Request To Exit (REX) Device – a device or sensor used to signal the system that passage through a secured door or gate in an unrestricted direction is requested.
g. System Manager – the person(s) having system rights to enroll Users, assign access privileges, generate system reports, and perform other duties
h. User – the holder of an Access Credential.

2. System Description

a. By presenting a compatible Access Credential card to a Reader, entering a code into a Keypad, or presenting to a Biometric Reader the system should identify an authorized User. Once the system identifies the User, it checks the pre-set authorization table to determine if the User is authorized for that opening at the current time and date. If the system determines that the User is authorized, a message is sent to the Door/Gate Control and Monitoring system (if the door/gate is a part of such a system) or sends a signal to a door control module. These then verify their own logic to determine if the door associated with the reader can be unlocked.
b. Some doors/gates may require a reader on both sides of the door assure authorized passage in both directions. Doors/gates allowing free passage in only one direction should employ a Request to Exit device on that side of the door/gate which should shunt the alarm function when movement in the free passage direction is sensed (and unlock the lock if necessary). Request to Exit devices include buttons, hardware with switches, passive infrared (PIR) detectors, photoelectric beam sensors, video motion sensors, etc.

c. The system should remember a specified number of events including the User, the door/gate accessed, date/time and at least 12 other parameters defined by the designer and the System Manager. This information is available for various audit purposes.
d. A minimum of 250,000 transaction events should be retained. The system should report when 75% of the on-line storage capacity is reached, and again when 90% of the on-line storage capacity is reached. If the on-line storage is not restored by manually moving the data to off-line storage before 100% on-line capacity is reached, the system should revert to "first in – first out" type housekeeping.
e. System User information is retained indefinitely.
f. All information in the database is available to provide practically any audit function. A few include:
    1) Entry/exit time/date for each User on a daily basis
    2) Current list of Users inside the facility by name, employee number, visitor number, etc
    3) Number of times each User has accessed each reader
    4) Number of times each User has attempted access at each reader during an unauthorized period
    5) Presentation of an impossible situation (same User at two widely separated doors within a short time)
    6) Last (1-5) (System Manager defined) doors accessed by a specific User with time /date
    7) Last (1-5) (System Manager defined) doors when access was denied a specific User with time/date
    8) Work assignment and identification issued to User
    9) And much more.
g. New systems are to be provided with a workstation to create or activate new Access Credentials, which if also serving as a badge, may have User's photo and other information. The workstation may also modify registration for existing Users, including de-activation and changes to access privilege. (Existing systems may or may not be provided with a workstation.)

3. Technology

a. The system is primarily software based, is expandable to enterprise level operation, and uses iCLASS, 96-bit (minimum) encryption.
b. No special workstation computer equipment should be required to run the system. The software should provide password access to a simple menu-driven interface allowing all administrative functions to be completed by persons with no special technical knowledge of computer systems. The system should record all changes to programming, user groups, or individual authorizations by logon.
c. The software should be configured to run continuously in the background, continuously on screen, or any combination.
d. Audit features of the software should be fully described. At least 12 different audit reports should be provided with the system, plus having a report writing sub-program to allow custom creation of any desired report using the available data.
e. Any type report can be printed by the System Manager using the information in the stored database.
f. System should be provided with the ability to manually or automatically call up a graphic map with flashing indicator at the sensor location upon receipt of an "out of range" signal from a monitored sensor.
g. User registration information should be manually entered and should include up to twenty-five (25) standard and System Manager defined fields. A minimum capacity for 500 users should be delivered with the system, which should be expandable to more than 10,000 users.

h. System should be provided with all required inputs and outputs projected to be required at the time of installation, plus an added 50% more unused inputs and outputs distributed throughout the system, for future use.
i. The system should be provided with all of the operating features and functions normally associated with these systems including the following:
    1) Global Anti-Passback
    2) Time and Attendance
    3) Time zones – 24 per day (min)
    4) Grouping – 100 groups min
    5) Video badging
    6) Custom badge design & production
    7) Audit reports
    8) Door open too long
    9) Door secure
    10) Third party interface
    11) Fast reader response – 250 milliseconds
    12) Fast system response – 500 milliseconds (including PLC throughput where applicable)
    13) Supervised & Fail-secure circuiting
j. Subject to the requirements of these Guidelines, products of the following manufacturers are acceptable:
    1) Lenel Systems
    2) Schneider/TAC iNet Seven
    3) AMAG
    4) Maxxess Systems
    5) Owner approved

4. Installation
    a. All Access Control system equipment, including Door Control Units, should be installed in secured, Security Electronics Equipment Room(s), and be grounded in accordance with requirements found elsewhere in these Guidelines.
    b. All control and monitoring equipment should be provided operating power from a UPS connected to a generator backed source.
    c. Program graphical maps and pages associated with the system. Use English names for all devices and locations. Copy the configuration files and deliver to the Owner's designated System Manager.
    d. Train the System Manager in the proper operation of the system, and demonstrate by registering up to fifty (50) system users and creation of up to fifty (50) Access Credentials in the presence of the Owner's System Manager.
5. Operations
    a. Users are initially registered and provided an Access Credential (if applicable) and/or keypad code, and/or their biometric information is stored. Conversely, Users and related privileges can be de-activated or otherwise altered at the designated workstation.
    b. Once a User is identified as authorized and the system clears the User of other parameters (time of day, etc) a signal is sent to the door/gate control and monitoring system (if present) or to a door control module. The control and monitoring system or door control module receives this request to unlock a door/gate and verifies its own logic (interlocking, time, lockout, etc) before actually unlocking the door/gate.

c. Every event on the access system including registrations, programming, clearances, grouping, reader cycles, keypad entries, authorizations to open door/gate, rejections to open door/gate, etc is recorded and stored in the data base and remains accessible for audit purposes.
d. The system operations are "severable" in that loss of communications with the main server only stops updates to the local door control module. The local door control module continues to operate and record activity until communications are restored with the server. Past Users will be able to access areas for which they are authorized. Newly enrolled Users will not be recognized and centralized alarms will not arrive at the control point until communications are restored with the server.

6. Performance Testing
   a. After completion of programming and installation, prove proper system operation by first registering the first fifty (50 Users then demonstrating correct operation at each reader, door/gate, monitor and request to exit device. After the demonstration, print at least three (3) different reports based on the just completed demonstration.
   b. Fully install, test and demonstrate the system. Prove the interface with other systems. Test each reader, keypad and other system device.

K. Operator Interface (Human-Machine Interface)

1. System Description
   a. The human machine interface (HMI) shall be composed of a touchscreen monitor connected to a computer to drive the display graphics. The HMI shall be interfaced into the PLC network to facilitate operator control and monitoring of the Security System. The HMI shall include the software to display the graphics on the touchscreen display, and an optional-use optical mouse.
2. System Performance
   a. Screen updates 250 milliseconds or less
   b. Command response 200 milliseconds or less
3. Acceptable Technology
   a. Surface Acoustic Wave
   b. 19 inch screen size minimum LCD display, 1,600 x 1,200 dpi minimum resolution
4. Installation Standards
   a. WSDOC TDIS for pathways and networked systems.
5. Performance Testing
   a. Shop test typical operations on 100% system mock-up including sample field devices
   b. 100% field functional test
   c. Verify response time
6. Acceptable Manufacturers
   a. Touch Screen Control Computers
      1) Touch screen
         a) Elo Touchsystems
      2) CPU
         a) Dell
         b) HP
      3) Software
         a) Vijeo Citect
         b) Owner Approved Equal

L. Qualifications of Security System Contractor

1. Responsibility Criteria

The Security System Designer should work with the DOC project manager to craft Responsibility Criteria, for the Owner's post-bid review process, that will determine:

a. That the Security System Contractor is a fully qualified security systems integrator with the requisite experience, in-house skills, and sufficient staffing, and
b. That he can demonstrate a history of success in the integration and installation of correctional facility Security Systems of the type and complexity of the project, and
c. That he has sufficient facilities and is capable of performing a full-performance test ("bench test") in his shop for all of the equipment to be delivered to the project, and
d. That he is capable of providing responsive warranty period support as described in these Guidelines.

VI. Construction Implementation

A. Post Award Conference

This Conference is to be held to assure that the Security System Contractor has interpreted the documents in the same manner intended by the Security System Designer. It offers the opportunity not only for an exchange of questions and answers, but also to consider alternate ways to accomplish the design goals and requirements, and/or to consider and discuss any substitutions that may have been presented by the contractor, based on his experience.

The Conference is held at a mutually agreed time and location after contract award. Attendance is required by the Security System Contractor and the Security System Designer. Attendance is recommended for the Owner, General Contractor, Prime Consultant, etc

At the conclusion of this Post Award Conference the contractor should be clear on how to proceed and what will be expected. All questions should be resolved, and the joint project review will be completed.

B. Shop Drawing Review Conference

This Conference is to be held to avoid multiple exchanges of technical and detailed documents, while assuring mutual understanding of the Security Systems. This Conference again offers an opportunity to assure a good understanding by the Security System Contractor, and to discuss any remaining questions or concerns he may have with the project work.

The Conference is held at a mutually agreed time and location approximately two (2) weeks after complete shop drawings are submitted. This gives the Security System Designer time to review the shop drawing submittal before the Conference.

Attendance at the Conference is required by the Security System Contractor and Security System Designer. Attendance is recommended for the Owner, General Contractor, Prime Consultant, etc.

At the conclusion of this Shop Drawing Review Conference all shop drawing issues are to be resolved and any follow-up items and their responsibility clearly understood.

C. Pre-Installation Demonstration (Bench Test)

This demonstration is held at the Security System Contractor's facility to assure that the system is fully functional after it has been fully assembled, and tested by the Contractor but before it is shipped to the project site. This demonstration affords the Security System Contractor the ability to troubleshoot and remedy any operational issues that can be identified before the system is shipped to the project. This also assists in troubleshooting in the field, since hardware and software demonstrated to work correctly in the shop likely means problems at the site are almost always resolved by field wiring and connection adjustments.

The Video Security System shall be fully configured with at least one (1) of each type of camera connected. To the greatest extent possible all network switching devices shall be connected in the manner they will be installed. The intercom and paging systems shall be assembled and configured, with representative stations and speakers connected. Contractor may simulate locking hardware, limit and position switches, sensors, etc, but not workstations or HMI's, to accomplish this full functional system test and demonstration.

This demonstration is held at a mutually agreed date and time. Attendance is required for the Security System Contractor and the Security System Designer. Attendance is recommended for Owner, Project Manager, facility Custody staff (preferably a security system control operator), facility Plant maintenance staff (including preferably an Electronics Technician), the General Contractor, the Prime Consultant, etc.

Touchscreen HMI layouts and nomenclature are usually fine-tuned by Owner and the Security System Designer. Owner's designated staff may be present to operate the system for the first time, and can provide additional input and suggestions for improvement.

Upon completion of identified changes, and correction of any problems by the Contractor (significant issues may require re-testing, as determined by the Security System Designer), the equipment is accepted for shipment to the project site.

D. Spare Parts

In most cases, the minimum spare parts complement should be as is recommended by the manufacturer. The Security System Designer should provide for those and any additional requirements in each specification Section, delineating the number and type of spares to be furnished.

Generally, at least one of each type of the following should be included:

1. Circuit board
2. Power supply
3. PLC I/O modules
4. Control workstation/server; complete
5. Video camera
6. Video workstation/server; complete
7. Encoder (if external)
8. Hard panel devices
9. Fuses
10. Intercom station
11. Intercom amplifier
12. Paging speaker/horn
13. Paging amplifier or amplifier module
14. Access Control reader
15. Access Control Keypad
16. Cold, configured PLC

Emphasis should be given to assuring that components that are difficult to obtain on short notice, parts for critical systems that could have a substantial impact on operation of the facility, and items known to have a short useful life, are included on the required spares list in appropriate quantities.

Spare parts should be kept in one secure location, be matched against the required spare parts list in each specification Section, and be inventoried by the Security System Contractor. When all required spares are assembled, Contractor should deliver the inventory list to the Security System Designer who should review it against the requirements. Any deficiencies should be corrected.

The Designer should then physically observe that all the inventory is actually in the spare parts location. Once the Designer verifies everything is accounted for, Contractor may deliver all spares, at one time, to Owner and obtain a signed detailed receipt for same, to become part of the project closeout.

E. Start Up and Commissioning

Before beginning this process, the Security System Contractor should complete the installation, verify system wiring, check fuses/circuit breakers, test as many individual components as possible, and prove communications.

The systems are started and operation is fully checked by the Security System Contractor in cooperation with the detention hardware and devices installer, especially with regard to setting limit switches and position switches.

A Punchlist visit is scheduled and completed by the Security System Designer. The Contractor completes any noted items and the Designer returns to back-check Contractor's final resolution of all items.

Contractor demonstrates all functions of all systems to Designer and Owner's representatives and trainers as final proof of compliance with documents. Deficiencies are noted and corrected as the testing proceeds. Specific attention should be given to operations after power interruption and after restoration of power.

Correction of all deficiencies allows that the Security System is now ready to turn over to Owner for beneficial use.

F. Training

Time for each training session is to be specified in the project manual in each specification Section having equipment and/or systems needing training.

Provide for training sessions to be held at the facility in a location to be determined by the Owner, at a date and time agreed upon in advance. Training sessions should cover both operation and maintenance of the systems and related equipment. When multiple levels of operation (ex: standard user/operator and supervisor levels) are required, specify separate training. Verify with the Owner how many work shifts should receive operator training.

For major systems, Security System Contractor should arrange for the manufacturer/vendor to deliver the training through its own qualified trainers, to present the training syllabus, which is supplemented by the Contractor for installation-specific issues.

Verify with the Owner the extent of training needed, and the number of staff requiring training. For higher levels of system competence, including manufacturer certification, training provided in the vendor's facility may be most appropriate. In those cases consider having Training Vouchers provided under the construction contract entitling the Owner to the training, for Owner's use at a convenient time which may be post-closeout.

For all required training, the Contractor should generate a training syllabus and obtain acceptance by the Security System Designer. Contractor should then propose a training schedule.

Professional-quality audio/video recording of each type of onsite training session should be created as a Contractor responsibility, and be provided to Owner on media and in format desired as part of the project closeout.

VII. Systems Maintenance and Support Post-Construction

A. Warranty

Provide that the Security System Contractor's warranty for the Security System work shall be for two (2) years from the date of project Substantial Completion as established by the Owner, and include all materials, products, equipment, and workmanship, without exception.

Stipulate that the Contractor shall return to the site and meet with the Owner's representatives and the Security System Designer approximately thirty (30) days before expiration of warranty period, for the specific purpose of confirming proper operation of the Security Systems installed. The Contractor is to promptly complete any required corrective work identified, even if the warranty end date subsequently passes.

B. Owner Rights During Warranty Period

Allow for Owner's staff to, at any time after acceptance of the project but while the Contractor's Warranty is in effect, to make normal adjustments to front panel accessible controls of any equipment, without voiding or having any negative impact on the contractor's warranty obligations.

The Owner may, from time to time, install Operating System security patches released to the public, and Anti-Virus software updates, without affecting the Contractor's warranty.

Also, the Owner may troubleshoot and attempt basic corrective actions within the bounds explained during the technical training sessions, and may, but is not obligated to, assist the Contractor by accomplishing any tasks as requested during a telephone conversation with Contractor's technical staff. Such efforts shall not in any way void the Contractor's warranty obligations.

C. Security System Contractor Warranty and Support

To ensure consistency and validity of communications the Security System Contractor should only accept trouble calls and communicate with regard to any aspects of the Security System only with individuals on a list of Owner's staff as agreed upon as part of the Closeout procedure. Owner representatives should call and speak only to Contractor's service staff as identified on the list.

1. Security System Warranty Service and Support

   Require that the Security System Contractor have a 24/7/365 telephone number to receive support and service calls. Contractor shall provide live response to telephone calls for assistance from the Owner's authorized representative within four (4) hours.

   If the issue cannot be resolved during the call, the nature of the issue should be categorized and be mutually agreed to by the Owner's representative and the Contractor's service representative as "critical" or "standard" for response prioritization. Both parties should record the essential elements of the communication.

   - If it is determined that a visit to the facility is required, the Security System Contractor shall dispatch qualified technical staff. Dispatched technician's travel should begin no later than four (4) hours after the call if the situation is "critical". Arrival at the site should be expeditious, and be coordinated with the Owner's representative to ensure access to the site.
   - If the situation is classified "standard" Contractor shall arrive at the site as agreed with the Owner's representative, but not later than on the second business day following the trouble call.

Spare parts delivered to the Owner through the project requirements may be used for warranty service work but shall not be used as a permanent solution to necessary repairs/replacements during the warranty period. Contractor shall replace Owner's spare parts as soon as practical at no cost.

If the required part is not available in the Owner's stock, or from the Contractor's inventory the Contractor shall order the part on the same day it is identified as necessary, and shall pay for next day delivery via an overnight carrier (FedEx, UPS, etc).

2. Security System Contractor Access to Security System Network

   Physical access to the Security System equipment locations is only with facility staff escort.

   Secure Network access via WAN (internet connection) that is compliant with DOC and ISB standards

3. Software Updates and Security Patches – by Security System Contractor

   During the warranty period the Security System Contractor shall test all general-release operating system security patches and updates within two (2) weeks of open release date for adverse interaction with the installed Security System hardware or applications. Any concerns shall be communicated directly to the Owner's individual or group tasked with supporting and updating the Security System.

   Application software updates and patches shall be provided and installed by the Security System Contractor for the first two (2) years after the Security System is commissioned. After two (2) years the Owner will either enter into a support and maintenance agreement, or will self-maintain the Security System.

   Coordinate with Owner for specific change control procedures and documentation.

   Applications software shall be maintained to be within two (2) released versions from the most current release.

   Security System Contractor shall be responsible for notifying the Owner of available system updates, and for scheduling installation activities.

   Update software and the installation methodology shall be tested by the Contractor in an off-line environment prior to implementation onto WSDOC's operational systems. Provide a copy of the update(s) to the Owner immediately upon its installation.

   Contractor shall be responsible for preserving existing data and configurations, and be able to restore updated software to the previous stable state, in the event of an upgrade failure.

4. Software Updates and Security Patches – by Owner

   Operating System security patches and updates shall be provided and installed by the owner.

   Anti-Virus software updates shall be provided and installed by the Owner.

   The Owner will define and maintain a change control process for implementing updates, changes and new configurations to network and computer based security system components.

VIII. Exhibits and Examples

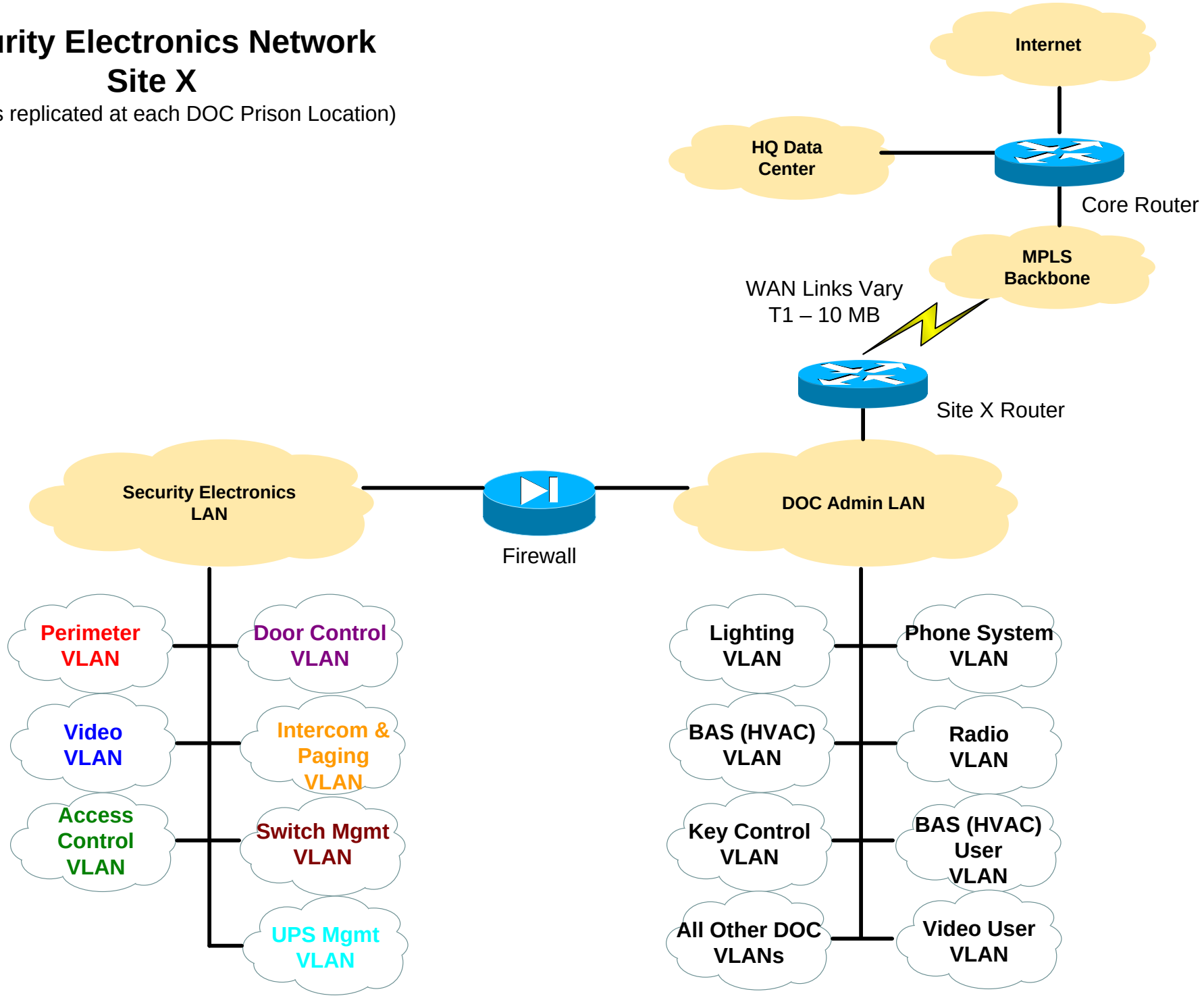
A. Security Electronics Network Diagram

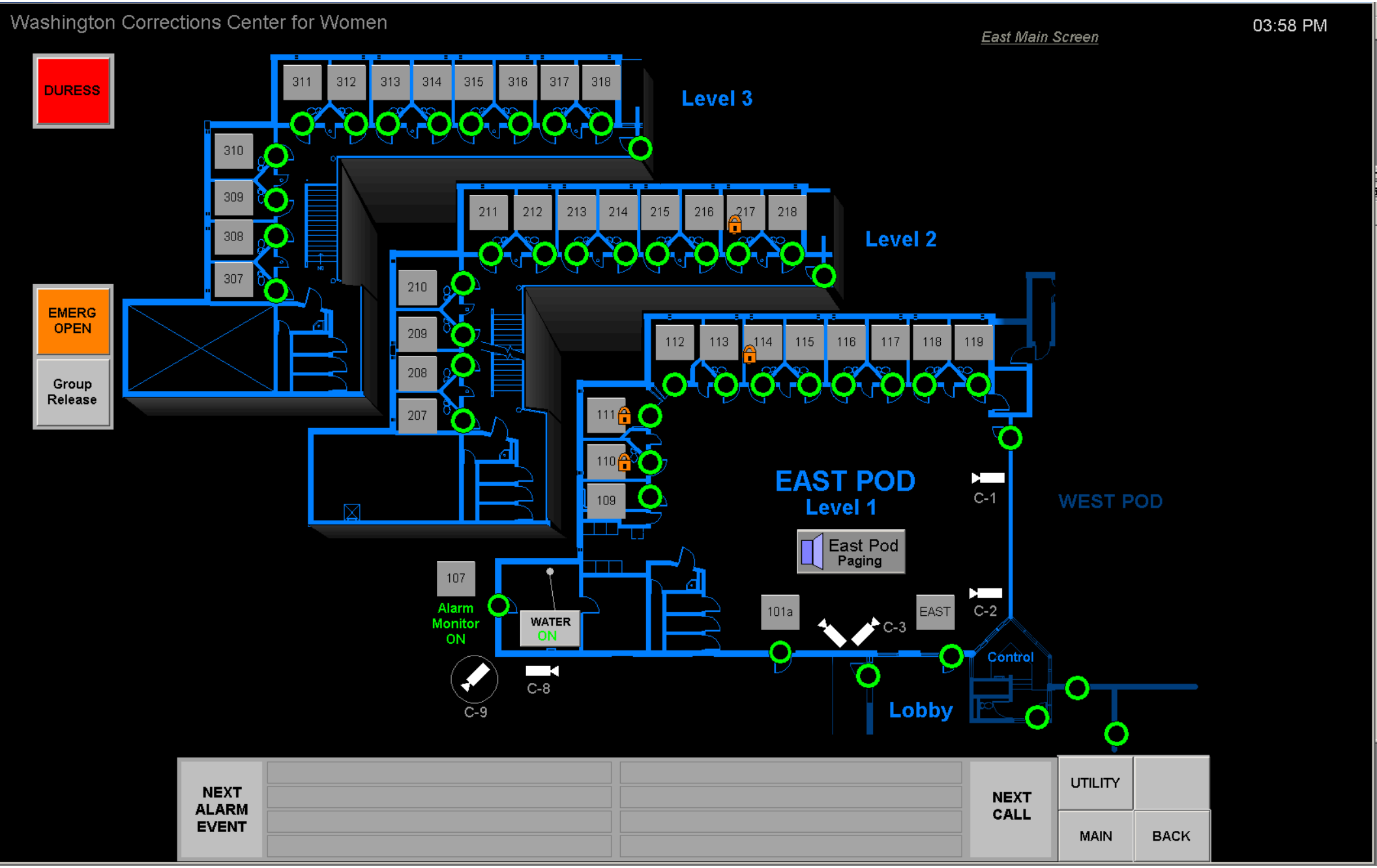
B. Example Touchscreen HMI Screenshots

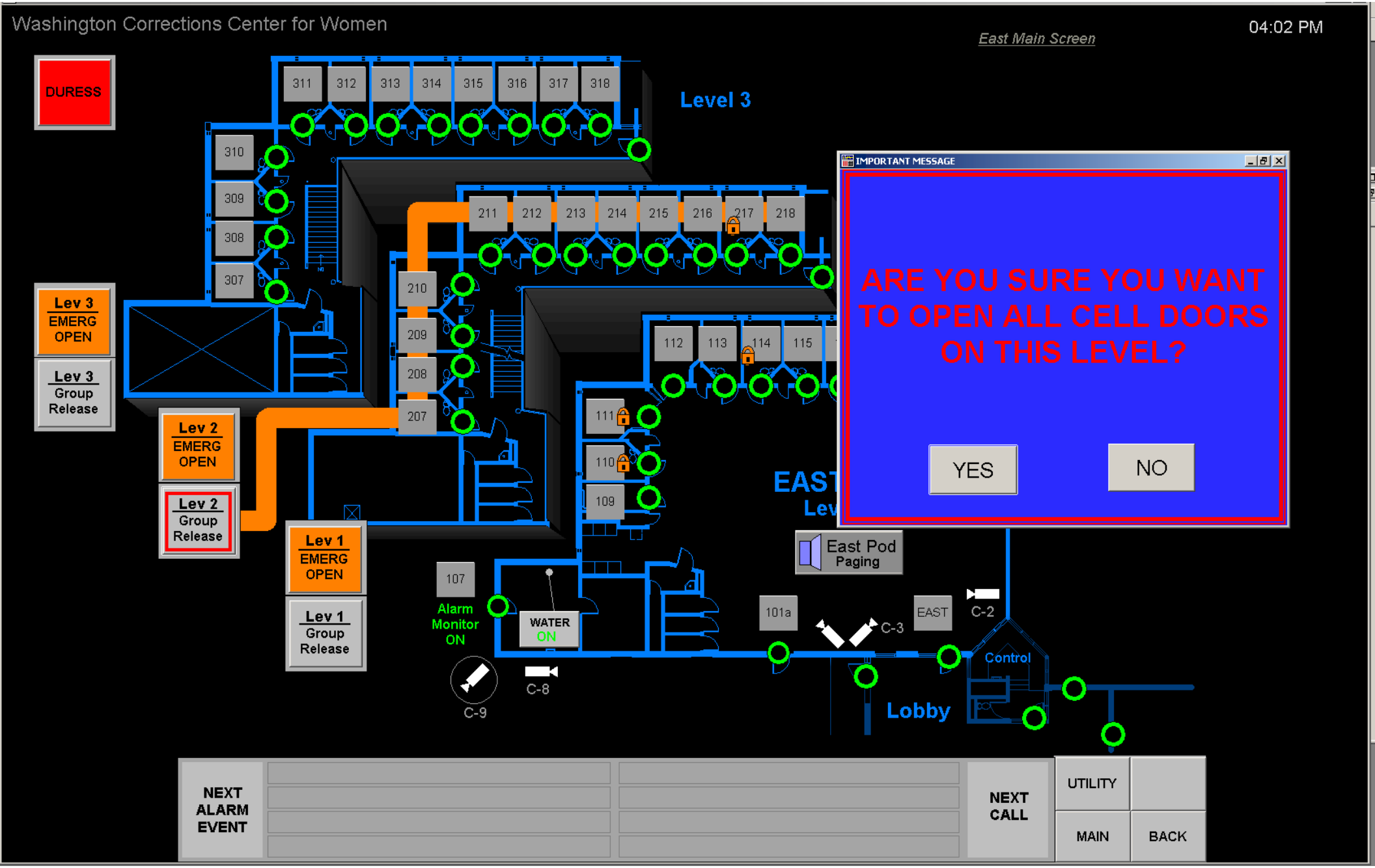
C. Example Touchscreen Operational Narrative

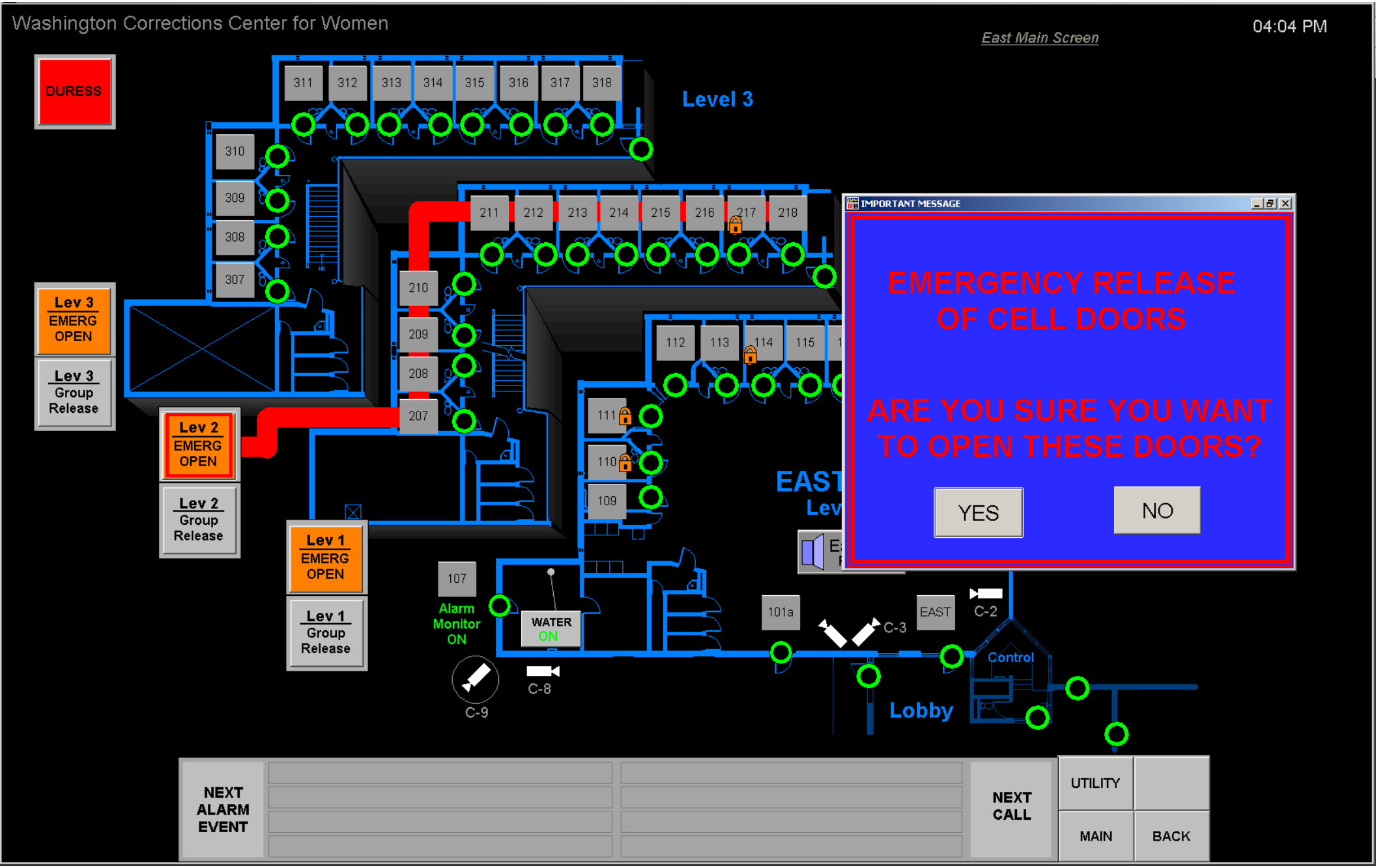
Security Electronics Network
Site X

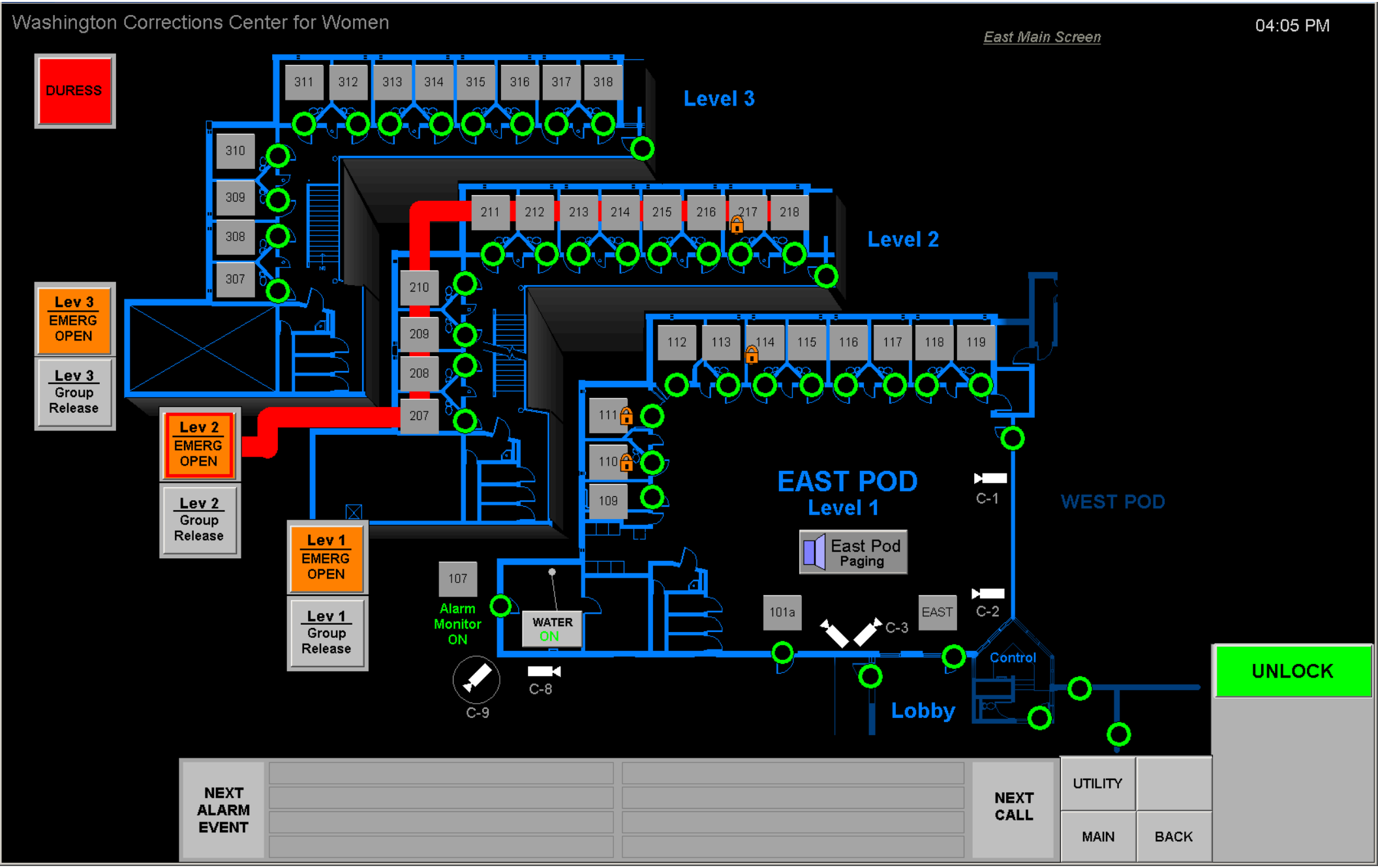
(Design is replicated at each DOC Prison Location)

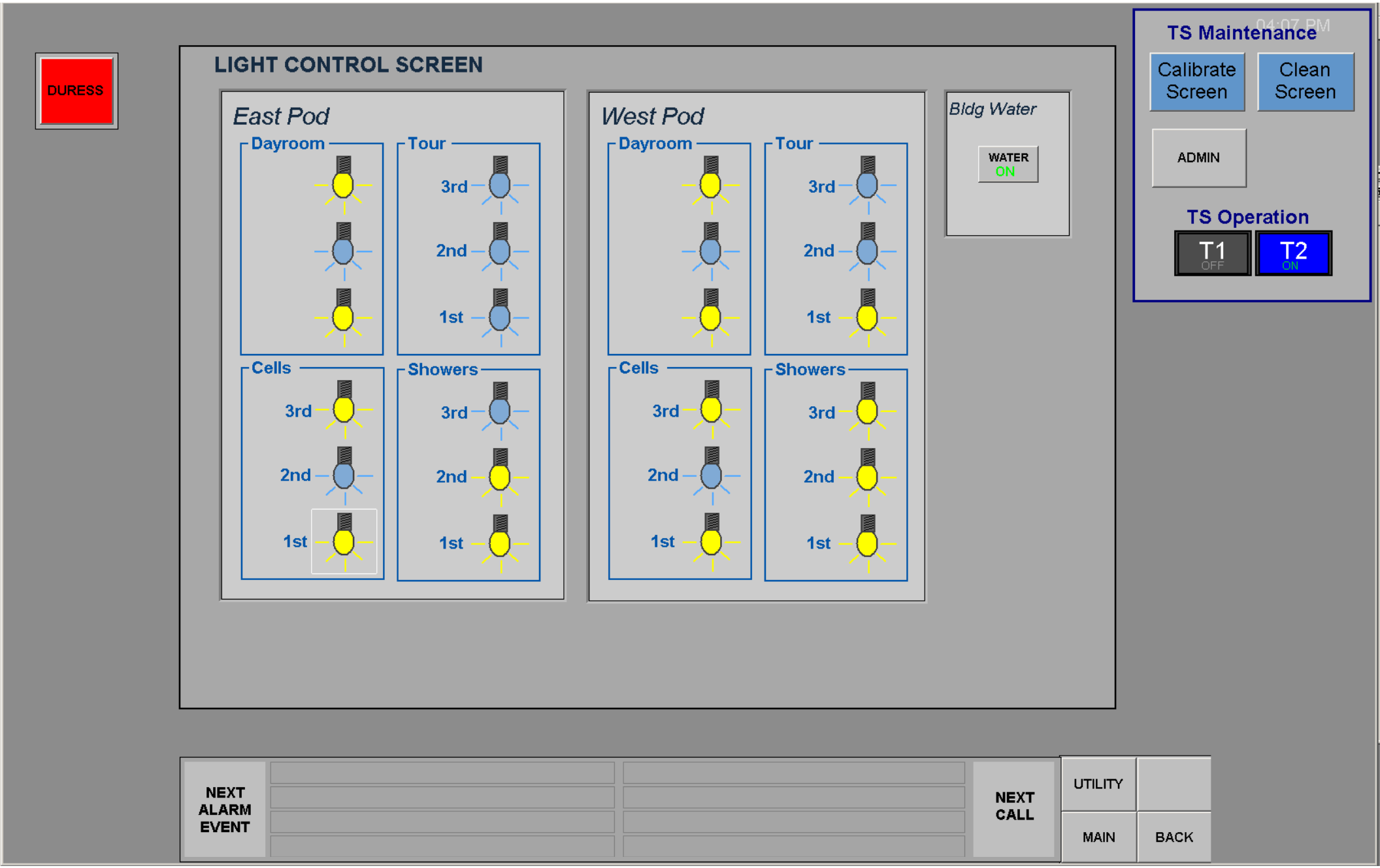


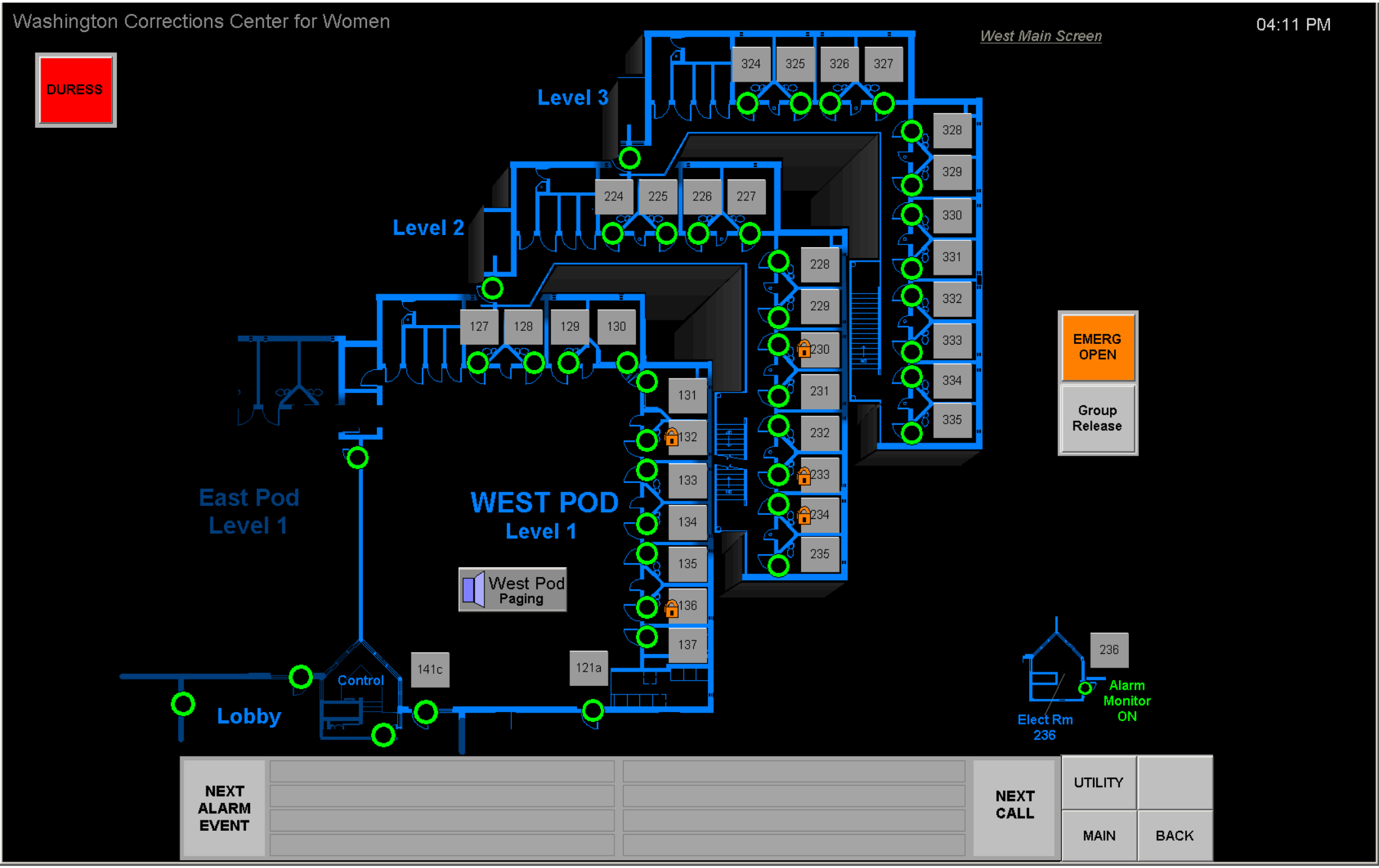

Washington Corrections Center for Women
East Main Screen
03:58 PM
DURESS
EMERG OPEN
Group Release
Level 3
Level 2
311
312
313
314
315
316
317
318
310
309
308
307
211
212
213
214
215
216
217
218
210
209
208
207
112
113
114
115
116
117
118
119
111
110
109
EAST POD
Level 1
C-1
WEST POD
East Pod Paging
107
Alarm Monitor ON
WATER ON
101a
C-3
EAST
C-2
Control
C-8
C-9
Lobby
NEXT ALARM EVENT
NEXT CALL
UTILITY
MAIN
BACK

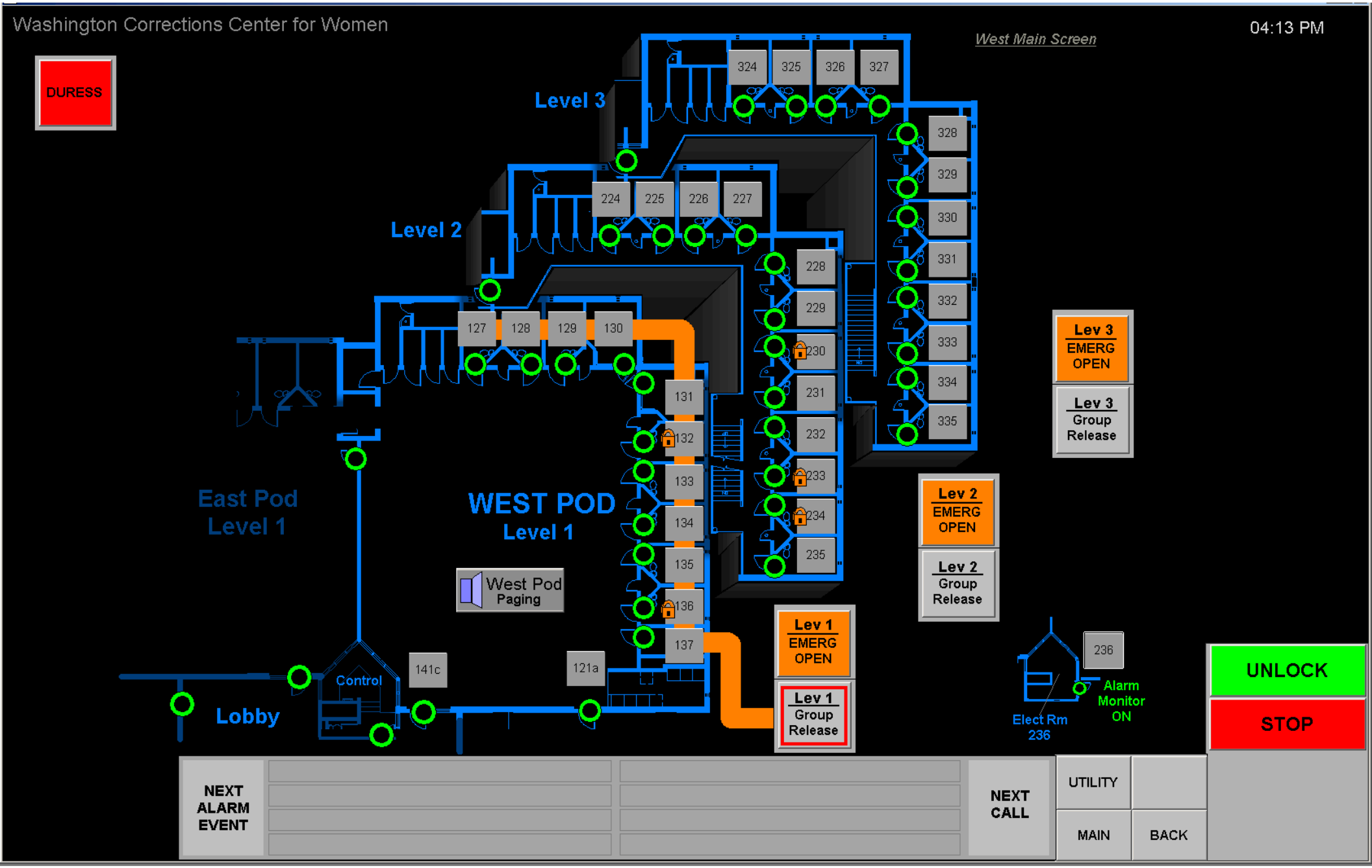

Washington Corrections Center for Women
East Main Screen
04:02 PM
DURESS
Level 3
311
312
313
314
315
316
317
318
310
309
308
307
211
212
213
214
215
216
217
218
210
209
208
207
112
113
114
115
111
110
109
Lev 3 EMERG OPEN
Lev 3 Group Release
Lev 2 EMERG OPEN
Lev 2 Group Release
Lev 1 EMERG OPEN
Lev 1 Group Release
IMPORTANT MESSAGE
ARE YOU SURE YOU WANT TO OPEN ALL CELL DOORS ON THIS LEVEL?
YES
NO
EAST
Lev
East Pod Paging
107
Alarm Monitor ON
WATER ON
C-9
C-8
101a
C-3
EAST
C-2
Control
Lobby
NEXT ALARM EVENT
NEXT CALL
UTILITY
MAIN
BACK


Washington Corrections Center for Women
East Main Screen
04:04 PM
DURESS
Level 3
311 312 313 314 315 316 317 318
310 309 308 307
211 212 213 214 215 216 217 218
210 209 208 207
112 113 114 115
111 110 109
Lev 3 EMERG OPEN
Lev 3 Group Release
Lev 2 EMERG OPEN
Lev 2 Group Release
Lev 1 EMERG OPEN
Lev 1 Group Release
IMPORTANT MESSAGE
EMERGENCY RELEASE OF CELL DOORS
ARE YOU SURE YOU WANT TO OPEN THESE DOORS?
YES
NO
EAST
Lev
107
Alarm Monitor ON
WATER ON
C-9
C-8
101a
C-3
EAST
C-2
Control
Lobby
NEXT ALARM EVENT
NEXT CALL
UTILITY
MAIN
BACK


Washington Corrections Center for Women
East Main Screen
04:05 PM
DURESS
311
312
313
314
315
316
317
318
Level 3
310
309
308
307
211
212
213
214
215
216
217
218
Level 2
210
209
208
207
Lev 3
EMERG
OPEN
Lev 3
Group
Release
Lev 2
EMERG
OPEN
Lev 2
Group
Release
Lev 1
EMERG
OPEN
Lev 1
Group
Release
112
113
114
115
116
117
118
119
111
110
109
EAST POD
Level 1
WEST POD
C-1
East Pod
Paging
107
Alarm
Monitor
ON
WATER
ON
101a
C-3
EAST
C-2
Control
C-8
C-9
Lobby
UNLOCK
NEXT
ALARM
EVENT
NEXT
CALL
UTILITY
MAIN
BACK


DURESS
LIGHT CONTROL SCREEN
East Pod
Dayroom
Tour
3rd
2nd
1st
Cells
Showers
West Pod
Bldg Water
WATER
ON
04:07 PM
TS Maintenance
Calibrate Screen
Clean Screen
ADMIN
TS Operation
T1
OFF
T2
ON
NEXT ALARM EVENT
NEXT CALL
UTILITY
MAIN
BACK

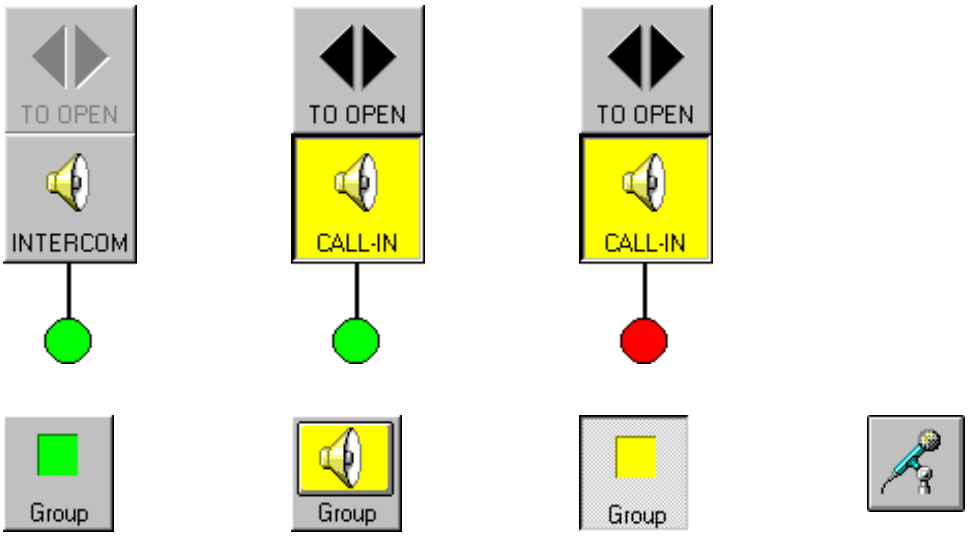

Washington Corrections Center for Women
West Main Screen
04:11 PM
DURESS
Level 3
Level 2
324
325
326
327
328
329
330
331
332
333
334
335
224
225
226
227
228
229
230
231
232
233
234
235
127
128
129
130
131
132
133
134
135
136
137
EMERG OPEN
Group Release
East Pod
Level 1
WEST POD
Level 1
West Pod
Paging
Control
141c
121a
Lobby
236
Alarm
Monitor
ON
Elect Rm
236
NEXT ALARM EVENT
NEXT CALL
UTILITY
MAIN
BACK


Washington Corrections Center for Women
West Main Screen
04:13 PM
DURESS
Level 3
Level 2
East Pod
Level 1
WEST POD
Level 1
West Pod
Paging
Lobby
Control
141c
121a
324
325
326
327
328
329
330
331
332
333
334
335
224
225
226
227
228
229
230
231
232
233
234
235
127
128
129
130
131
132
133
134
135
136
137
Lev 3
EMERG
OPEN
Lev 3
Group
Release
Lev 2
EMERG
OPEN
Lev 2
Group
Release
Lev 1
EMERG
OPEN
Lev 1
Group
Release
236
Elect Rm
236
Alarm
Monitor
ON
UNLOCK
STOP
NEXT
ALARM
EVENT
NEXT
CALL
UTILITY
MAIN
BACK

EXAMPLE – Touchscreen Operational Narrative

System CD: Swing Movement Door with Intercom and Video Surveillance

Software Panel Graphics:



Software Panel Operation:

Communication may be requested by depressing the Call button at the door.

Functional group software panels: This starts the associated functional group's Group button flashing yellow and sounds the call-in tone. Selecting the flashing button will change the button to solid yellow, display the button as depressed, and silence the tone. The graphic representation of the door will appear in the primary or secondary functional area on the main software panel screen. If both functional areas contain graphics, selecting the flashing button will have no effect, until one of the two areas is cleared using the associated Return button. A graphic representation will show the door's current position (secure or not secure), intercom status (call-in or (in) active intercom), and display the name of the functional group. A Return button and Push-to-Talk button will appear.

All software panels: The call is answered by selecting the flashing yellow Call-In / Intercom button labeled "CALL-IN". The Call-In / Intercom button will change to solid yellow, display as depressed, and silence the tone. The operator may also select an intercom for a door with no call-in. In this case, the Call-In / Intercom button is the default button color and labeled "INTERCOM". When selected, the Call-In / Intercom button will display as depressed, and turn yellow. An audio and video communication link will be established to the door. The operator may then talk to the caller by depressing and holding the Push To Talk Switch (physical panel or foot switch). Releasing the switch will enable the operator to hear the caller again. The Push To Talk button on the software panel echoes the position of this switch.

The operator must select the depressed Call-In / Intercom button to cancel the call-in. The button will display in the up position, and in the default button color.

The Open Door button labeled "TO OPEN" will be disabled, and the door cannot be operated, until the Call-In / Intercom button is displayed as depressed.

The door may be unlocked by selecting the Open Door button. If any associated interlocked doors are unsecure, this button will be disabled, and the door will not unlock, unless the Interlock Override. Associated doors are interlocked and will not unlock if this door is unsecure, unless the Interlock Override is active. A graphic representation will show the current door position (green for secure, and red for unsecure) and will change to respond to the DPIS information to indicate changes in the secure condition of the door.

Where shown, this system disables the Door Status Alarm until the door is re-closed. When the door is again secure, the Door Status Alarm is again enabled.