

GROUP SECURITY MANAGEMENT

TRANSNET PHYSICAL SECURITY SYSTEMS STANDARD

Standard Number	TPSSS20/05/2016
Version Number	1.2
Effective Date	20 May 2016
Compliance Achieved By	6 months
Review Date	3 years

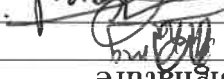
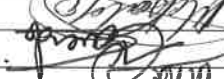
Recommended by Standard Owner and Standard Sponsor

I hereby acknowledge that a research has been conducted and that the Standard is not duplicated or in conflict with any other Transnet Standards.

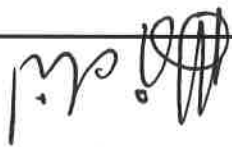
Name	Designation	Approval Signature	Date	E-Mail	Contact Number
Mfundisi Dumisa	Head: Technical Support		20/5/2016	Mfundisi.Dumisa@transnet.net	011-3081200
Rodney Toka	Manager: Security Management		20/5/2016	Rodney.Toka@transnet.net	011-3082233

Distribution list for consultation and recommendation

The Standard went through an extensive consultative process within Transnet for reviews, inputs, comments and recommendations. The table below lists all the fora that reviewed the document and recommended its adoption.

Forum	Chairperson	Recommendation Signature	Date	Email	Contact Number
ISF	Mandla Phakathi		18/07/2016	Mandla.Phakathi@transnet.net	011-3083032
AC	Kevin Goverder		21/7/2016	Kevin.Goverder@transnet.net	011-3083840
IRSGC	Tshepo Mabalayo		18/07/2016	Tshepo.Mabalayo@transnet.net	011-3083840

Final Approval



Name of Committee

Makene Mosele

Date Approved

8IMCO - BUSINESS INFORMATION MANAGEMENT SERVICES
27 / JULY / 2016

1. Introduction

The Transnet Physical Security Systems Standard (TPSSS) presented in this document is based on a Natcom written Transnet security systems standards, EIMS IT standards and policies, electronics and software engineering protocols and algorithms standardized by international software controlling bodies, mentioned in the document. The standard covers IP camera surveillance systems, Access Control, networks and related technologies associated with these systems.

2. The Case for Standardization - User Requirements

The need for security systems standardization within Transnet is to achieve the following:

- Effective use of technology across Transnet to enhance security.
- Shorter turn-around time and high productivity.
- High information availability.
- Information sharing and distribution across ODS/SBUs.
- Data integrity and consistency.
- Economies of scale to reduce cost of security within Transnet.
- Exploiting sheer size of Transnet and its buying power.
- Better and advance technology implementation in future building from current large scale experiences.
- Laying the foundation for Transnet long term security systems strategy.

3. Scope

In the context of this document, Security Systems refer to electronic access control systems, IP camera surveillance systems (previously called Closed Circuit Television (CCTV)) and related subsystems.

The Security Systems Standard applies to all Security Systems installed by Service Providers and used within Transnet Operating Divisions (ODs) and Strategic Business Units (SBUs). The Standard shall take effect on the day it is signed-off as approved by the highest approving authority within Transnet. All systems designed and installed after the signed-off approval date shall comply fully with the standard. Systems that are in the process of being designed or whose designs have been completed but physical installation has not begun on the day the standard is signed-off as approved, shall comply with the standard.

The Standard shall not apply to the following systems:

- legacy and already installed systems
- systems whose physical installation has already begun

4. Definitions and Abbreviations

Security Systems	Electronic and software based systems used in physical security; e.g. Camera surveillance systems, CCTV, Access Control and associated sub-systems.
IP camera	Network camera
HD	High Definition - megapixel resolution with aspect ratio of 16:9.
Onvif	Open Network Video Interface Forum - an international body facilitating the development and use of open standards for the interface of electronic, software and IP based products used in security.
PSIA	Physical Security Interoperability Alliance - an industrial standardization initiative developing standards and promoting the interoperability of IP-based security devices based on these standards. It is a competitor to Onvif.
VMS	Video Management Application Software - an application program controlling the entire camera surveillance system.
AMS	Application Management Software - an application program managing and controlling the entire Access Control System.
Time Synchronization	Making computers and devices on the network to indicate the same time.
Intelligent Video	- "the process of analyzing video data with the goal of transforming it into actionable information.", (Nilson, 2009, p.274)
Intrusion Systems	These are subsystems of the main systems that detect unauthorized entry and report to the main systems.
Pre-alarm buffering	Continuous recording for the last x or y seconds.
ISO	International Standards Organization also referred as International Organization for Standardization.
IEC	International Electrotechnical Commission.
ANSI	American National Standards Institute.
IEEE	Institute of Electrical and Electronics Engineers.
OEM	Original Equipment Manufacturer, designer, engineer and developer of the product
IT	Information Technology
ISF	Information Security Forum
AC	Architecture Council
IRSGC	Information Risk, Security, Governance & Compliance

5. IP Camera Surveillance System

5.1. Architecture

The Surveillance System shall be based on IP, High Definition (HD) cameras and shall run on x86_64 architecture, with cameras fully supporting the architecture.

5.2. Software

1. *Architecture:* x86_64. This applies to CPU, hardware, OS and application programs and will ensure large directly addressable memory space of 2^{64} and faster processing of multimedia data.

2. *Onvif or PSIA standards:* Video Management Software must be 100% Onvif (Onvif v2.0 or latest stable) or PSIA (CSC v1.0, IPMD v1.1, RACM v1.1a, VAS v1.0, CMEM v1.0 or latest stable) compliant for image display, playback, management, manipulation and configuration.

3. *Display media:* Supported video resolution of up to 16MP (4872x3248).

4. *Web interface:* Video management must support accessing and managing video online with appropriate web browsers, using proper safeguards. Cameras and video encoders shall have built-in web interface to facilitate remote web access to video.

5.2.1 Video Management Application Software (VMAS)

1. Operating Systems (OS):

- Multitasking
- Multiprocessors and multiprocessing
- Scheduling
- TCP/IP network support and network aware
- Quality of Service Support
- Strong security feature support
- Support for 64-bit architecture

2. Application Management Software:

- Development toolkits: ANSI C/C++ (C11 and C++11), Java 7 SDK, C#. Native applications are highly recommended
- Client-Based: client application "is installed on a server that is separate from the recording server where management software is installed.", (Nilsson, 2009, p.247)
- Web-Based: supported by a web-server, video management software is installed on a PC platform that is used for recording.

3. Application Management Software Functional Characteristics:

- *Manage cameras*: Video management software shall provide the ability to add and configure basic camera settings, frame rate, resolution and compression formats. It shall also provide camera discovery and complete device management.

- *Video recording*: Support for continuous recording, recording on trigger and on schedule recording. Video format shall be based on MPEG-4 latest stable version.
- *Audio Recording*: Support for audio recording either as built-in functionality in a network video product or through video management software. Audio shall be synchronized with video with time-stamping on both audio and video packets.
- *Video indexing* : Recommended file systems shall be NTFS and ext4. All available video shall be indexed in a database to facilitate;

- shared access
- data integrity
- efficient search and
- direct access

- *Advance search*: Video management software shall support advance video search using date and time, area or motion-based search.

- *Exporting Files*: Video management software (be it proprietary, free or open) shall enable users to export recorded video to standard file formats such as Audio Video Interleave (AVI), Advance Streaming Formats (ASF0, etc.

- *Viewing* : Video management software shall provide for the following types of viewing;

- live viewing
- play back
- multi-streaming

- *Mapping Functionality* : For easier camera selection by operators and better display of alarm events, video management software shall provide mapping functionality.
- *Event Management* : Full handling and management of events which may be triggered by;

- input ports
- manual trigger
- video motion detection
- audio trigger
- temperature
- camera tampering

and handle responses to events by one or a combination of the following;

- Uploading images for recording at certain frame rates, for certain duration, at certain bit-rate of affected areas
- Activate output ports
- Send e-mail notifications
- Send HTTP of TCP notifications
- Go to a PTZ preset

1. *Surge protection*: All camera shall be fitted with surge protection against possible lightning and electrical interference.
2. *Camera lens*: The system shall support camera lenses ranging from less than 21mm to 300+ mm, depending on the area of application and the required image quality.
3. *Compliance to Onvif and/or PSIA standard*: Cameras used must be 100% compliant to Onvif or PSIA IP camera standards. The applicable versions of these standards are specified in "5.2.2".
4. *Electronic Image Stabilization (EIS)*: All outdoor cameras deployed in areas with high vibrations and motion due to heavy machinery, traffic and wind shall be equipped with EIS to ensure that the quality of the image is unaffected by these movements.
5. *Presets and Guard Tours*: All PTZ (pan, tilt, zoom) (incl. PTZ dome) cameras shall support Presets and Guard Tours. The video management program shall support preset and guard tours settings and configurations.
6. *Privacy masking*: All PTZ (incl. PTZ dome) cameras shall support Privacy Masking.
7. *E-Flip*: PTZ cameras deployed in high risk areas must support e-Flip functionality.

5.3. Cameras

- *Audit log files*: Video Management Software shall provide audit log which presents a list of user actions based on user profile.
- *Event logs*: Video management software shall manage, handle and keep event logs that provide a list of events sources based on date, time, type, area and source. Event logs shall facilitate event search and playback.
- *Which authorized users have access to which cameras and components of the system and what actions can these users perform on the system.*
 - Administrator: access to all functionalities
 - * Operator: access to prescribed or defined functionality
 - * Viewer: access certain live cameras
- Which authorized users have access to which cameras and components of the system and what actions can these users perform on the system.
- Authorized users
- Passwords
- Different user-access levels, for example;
- * Administrator: access to all functionalities
- * Operator: access to prescribed or defined functionality
- * Viewer: access certain live cameras
- Which authorized users have access to which cameras and components of the system and what actions can these users perform on the system.
- *Security*: Video Management Application Software shall enable the following to be defined or set:
 - Authorized users
 - Passwords
 - Different user-access levels, for example;
 - * Administrator: access to all functionalities
 - * Operator: access to prescribed or defined functionality
 - * Viewer: access certain live cameras
- *Time synchronization*: The management application software shall provide time synchronization of all networked devices by using Network Time Protocol (NTP) server.
- Send an SMS with text information about the alarm or an MMS with an image showing the incident
- Activate an audio alert on the video management system
- Enable on-screen pop-up showing images from event source
- Show procedures that the operator should follow

8. *IR-blocking filter*: Cameras deployed in poorly lit areas at night must support IR-blocking filter or IR-cut filter. The switch from colour to black and white shall be automatic, as light diminishes and night sets in.

9. *IR Illuminators*: Where 24/7 monitoring is required in areas with low light and shorter distances to be covered, cameras supported by IR Illuminators shall be used for better images.

10. *Backlight Compensation*: All cameras shall support Backlight Compensation to managed contrasting brightness of the scene being monitored.

11. *Wide Dynamic Range*: All cameras shall support this feature to handle scenes with both extreme and dark areas at the same time.

12. *Day/Night Control*: This mode shall be automatic and manual to handle day and night conditions to ensure high quality video footage at all times of the day.

5.4. Support for Intelligent Video

The surveillance system shall support intelligent video (IV) based on the following categorizations

- Pixel-based IV applications
- Object-based IV applications and
- Specialized IV Applications

The system shall either support all categories, one or two of them depending on user requirements.

5.5. Pre-alarm buffering

The system shall support pre-alarm buffering. The time before and after an event shall be at least 30 seconds or more.

5.6. Monitors

Monitors supporting high definition (HD) video modes of 1080p and higher or ultra high-definition video modes of 2000p or higher, all of progressive scanning type, shall be used.

NB: *Original Equipment Manufacturer (OEM) different HD monitor specification may be acceptable.*

5.7. Compression

Supported compression standards range from H.264AV to H.265 or the latest stable version of these standards. The standard shall be supported by all front-end, middleware, back-end devices and software.

5.8. Recording and Storage

5.8.1 Video Management Platforms

Recording and storage system shall be based on the following video management platforms:

- Windows (current stable) with New Technology File System (NTFS)
- Linux (current stable version) with Fourth Extended File System (ext4) and or B-tree file system Btrfs) support.
- Any Operating System (OS) platform with the following characteristics:

- Job or process management
- Resource management
- Management of I/O devices
- Memory handling, allocation and management
- File handling and management
- Error reporting
- Resource protection
- Network management
- Multitasking and multicomputing

with continuous read/write and journaling file system support.

5.8.2 Video File Systems

Recorded video shall be stored as standard files e.g. JPEG, MPEG, AVI, ASF, etc. or as raw indexed data. *Open file formats* and *free file formats* shall also be used with *free file formats* **highly recommended**. The structure to store video shall be optimized for high recording performance, quick search, tampering detection, stability and recovery.

5.8.3 Hard Disk Drives

SCSI (Small Computer System Interface) hard drives, in terabytes of sizes, depending of the amount of data to stored and archived, with transfer rate of at least 640Mbps and Mean Time Between Failure (MTBF) of at least 1 million hours, are highly recommended.

Enterprise or OEM grade drives, in RAID 5 or RAID 6 configuration, as standardized by Storage Networking Industry Association (SNIA) in the Common RAID Disk Drive Format (DDF) shall be used.

5.8.4 On-Board Storage

All cameras shall have on-board memory that can be extended by an SD card or USB thumb drive for more storage. At least 8 hrs of continuous recording utilizing total camera storage size shall be possible.

1. *Power over Ethernet (PoE)*: Support for PoE shall be in accordance with IEEE 802.3af-2003 standard for fixed cameras and IEEE 802.3at-2009 standard (PoE plus) for PTZ cameras.
2. *Fixed IP addresses*: All network devices shall be allocated fixed (static) IP addresses.
3. *DHCP*: While the protocol must be supported, it will not be normally used to allocate and managed IP addresses. Its use will only be possible if it does not undermine the security of the system and it improves its performance.
4. *HTTPS*: To provide secure communication.

The following capabilities and functionality shall be provided by the network:

Logical topology: Ethernet based on 10-Gigabit Ethernet 802.3ae and 802.3an specifications or latest versions of these specifications.

speed.

Network medium: Glass fiber (fiber optic). All network (backbone and access) shall be based on fiber. Other network media type shall be utilized where fiber alone cannot be used. In such cases compatible media and conversion devices shall be used to maintain fiber transmission

Network model: Open Systems Interface (OSI) Model or TCP/IP Model.

All cables and network devices shall be protected against lightning damage.

5.9. Network

The primary recording system shall support automatic data archiving to keep footage for longer period. The size of the archiving storage shall be determined by amount of data to be archived and the period to keep data.

5.8.7 Data Archiving

Either both NAS (Network Attached Storage) and SAN (Storage Area Network) shall be supported or one of them is supported. Requirements shall dictate which storage system is utilized. However, SAN is recommended for its high speed, high throughput, scalability and redundancy.

5.8.6 Network Attached Storage (NAS) and Storage Area Network (SAN)

The primary recording system shall support Network Attached Storage and/or Storage Area Network, discussed below.

OEM specified and recommended network recorder (NVR) shall be one of the primary forms of recording, alternatively, PC server based recording as per OEM specifications and recommendations shall be used. The minimum size of a recording storage shall be at least 30 days of continuous recording at 25f/s of all installed cameras. The size shall be determined by the number of cameras, recording at 25f/s continuously for 30 days.

5.8.5 Primary Recording

5. *IP address filtering*: To enable defined IP addresses to have access rights to cameras.

6. *802.1X support*: To support port-based authentication.

7. *IPv6 Addressing*: To ensure compatibility with the next addressing standard in future.

8. *Full support for wireless technology*: The system shall be fully wireless capable by supporting 802.11 core standard and its extensions, viz;

- *The 802.11b Extension*
- *The 802.11a Extension*
- *The 802.11g Extension*
- *The 802.11n Extension*
- *The 802.11s Extension*

5.10. Audio

Audio devices and audio systems integrated into security systems shall support the following audio codecs;

- *Advanced Audio Coding - Low Complexity (AAC-LC)*. This is highly recommended although it requires a license.

- *Pulse-Code Modulation (G.711 PCM)*.

- *Adaptive Differential Pulse Code Modulation (G.726 ADPCM)*

- *Adaptive Multi-rate - Wideband (G.722.2 or AMR-WB)*

Audio and video synchronization shall be achieved through the use of MPEG-4 or H.264 or higher versions of these codecs. While Motion JPEG does time-stamp video, it may not always be supported in a network camera and is therefore not recommended.

5.11. Intrusion Alarm Systems

Intrusion alarm systems shall be based on audio/sound, motion, light, interruption, time, surrounding environment or layout of objects in an environment, forceful jerking of objects as agents to trigger alarm and be fully integrated to surveillance and access control systems. Support for artificial intelligent based event triggering is highly recommended.

In the event of alarms being triggered by occurrence of events described above, the system shall be able to send short messages by email, SMS, etc. to the recipients or destinations. The system shall support sending such messages through wired and wireless media. The destination and receiving media shall be both mobile and wired.

Intrusion alarm systems shall be supported at Camera Surveillance System and/or Access Control System level(s).

5.12. Security

1. *Encryption standard*: The supported standard is Advanced Encryption Standard (AES). The standard is recommended by the National Institute of Standards and Technology (NIST). "Until today, no crypto-analytical attack has the ability to crack the AES key.", (Nilsson, 2009, p.194). AES is also one of the encryption algorithms specified in Transport Cryptography Standard, (Transport Cryptography Standard, 2014, p.8).
2. *Areas for data encryption*: Support for data encryption on the cameras, storage (NVRs), viewing stations, systems administration stations and data distribution programs.
3. *Digital signature*: Recorded video and audio shall be digitally signed using 256-bit encryption standard or AES.
4. *SSL/TLS*: The system shall support Secure Socket Layer (SSL) and or Transport Layer Security (TLS) transmission to ensure privacy.
5. *Username and Password Authentication*: All log-onto the systems shall be through username and password and their authentication. Each username shall be associated with a profile defining what that user can and cannot do in the system. Password generation, management and use shall be as specified in Transport Cryptography Standard.
6. *IP Filtering*: All installations shall support IP filtering. Where higher level of security is required, this feature shall be activated.
7. *IEEE 802.1X*: To prevent "port hijacking", (Nilsson, 2009, p.227), the entire systems network and devices shall support this standard, with a dedicated authenticating server on the network. It is highly recommended that 802.1X be built into network cameras and video encoders. The following implementation of 802.1X shall be supported;
 - Temporaryftp://ftp.gnome.org/pub/gnome/sources/glib/2.40/glib-2.40.0.tar.xz Key Integrity Protocol (TKIP)
 - Pre-Shared Key (PSK)
8. *Wi-Fi Protected Access (WPA2)*: In WiFi environment WPA2 shall be supported.
9. *Hypertext Transfer Protocol Secure (HTTPS)*: At times it will be necessary to provide privacy on the data itself and not on the transport layer. This is achieved by the use of HTTPS.

6. Access Control Systems

6.1 Client/Server Principles

The Access Control System shall be based on client/server principles, with Access Control Applications Management Software (AMS) as a client and database systems performing and providing server functions to clients.

6.2 Proximity card

The Access Control system shall be based on proximity card technology, supporting both passive and active cards based on *ISO/IEC 14443* standard.

6.3 Card Readers and Controllers

Network based controllers shall have memory and processing power, to work independently of the access control server (host machine) in the event of network communication failure, to control access in their designated zones until network communication is restored.

Controllers based on RS-485 serial protocol, shall have memory and processing power, to work independently of the access control server (host machine) in the event of network communication failure, to control access in its designated zone until network communication is restored.

IP readers based access control system shall also be acceptable.

6.4 Biometrics

Biometrics technology used shall support proximity card standard, as described in "subsection 3.3"

6.5 Bar Coding Technology

Bar code scanners shall read/scan bar coded data according to international bar codes specifications ISO/IEC 15416 for linear bar codes and ISO/IEC 15415 for 2D bar codes.

Alternatively, the bar code scanners and bar code readers must be able to read/scan bar coded data on South African ID issued by Department of Home Affairs (DHA) and South African vehicle license disc issued by Department of Transport (DOT).

6.6 Access Control Application Management Software (AMS)

1. Operating Systems (OS):

- Multitasking
- Multiprocessors and multiprocessing
- Scheduling
- TCP/IP network support and network aware
- Quality of Service Support
- Strong security feature support
- Support for 64-bit architecture

2. Application Management Software (AMS):

- Development toolkits: ANSI C/C++ (C11 and C++11), Java 7 SDK, C#, Native applications are highly recommended
- Client-Based: Application Management Software must run as a client to the Access Control database server.
- Web-Based: Application Management Software shall support accessing the database server through a web-browser, if required.

3. Application Management Software Functional Characteristics:

- *Access Control Enrollment*: The entire enrollment process shall be handled by the AMS. The Access Control System shall provide local and remote enrollments. Both these type of enrollments shall be handled by AMS.
- *View Transactions*: Live and recorded access control badging shall be viewable from the AMS, locally and remotely.
- *Manage readers and Controllers*: The operations and administration of readers and controllers shall be provided by the AMS.
- *Manage and handle Bar codes*: The bar coding technology attached to the Access Control System shall be fully integrated into the System and managed by the AMS and administered through it.
- *Management and Control Boom Systems/Vehicle Barrier Systems* : Management, control and configuration of boom systems/vehicle barrier systems shall be provided by the AMS.
- *Deletion and data modification* : Deletion of data and its modification in Access Control database, controllers and readers shall be through AMS.
- *Querying the database* : By supporting executing SQL statements (SQL:2011) directly on the local database server or remotely, using Graphical User Interface (GUI).
- *Reports* : Reports in the following formats
 - text
 - tables
 - pie-charts
 - linear graphs
 - bar graphs
- shall be provided. Reports creation and generation shall be provided by AMS and execution of SQL statements (SQL:2011) on local machine or remotely.
- *Advance Search*: AMS shall support advance data search using any of the fields comprising individual tables in the database or a combination of the fields in one or more tables. Search shall also be conducted using date and time and a field or combination of fields across tables.
- *Exporting Files*: AMS shall enable users to export query results and reports to office applications, e.g. word processors, spreadsheets and presentation applications. Exportation to other widely used file formats like pdf, XML, HTML, and various graphics formats shall be fully supported.
- *Area Zoning*: Defining areas card bearers can and cannot visit.
- *Audit Trail and Anti-pass back*: Setting up and defining anti-pass back mechanism on the system and viewing card transactions shall be provided by AMS.
- *Data Distribution*: AMS shall support direct or remote data (reports and query results) distribution using email applications and web-browsers.
- *Time Synchronization*: The management application software shall provide time synchronization of all networked devices by using Network Time Protocol (NTP) server.

A copy of Systems Administrator and Operator user profiles shall be stored on the same machine backing up card and biometrics enrollment profiles, kept separate away from the Access Control server and client machines running the Access Control system on a daily basis. These profiles shall be updated periodically to stay current.

6.7.4 Operator and Systems Administration Profile Backup

A copy of the metadata of the entire Access Control database shall be stored on the card enrollment back up machine and be updated periodically according to the recent changes on the main server machines.

All card enrollment details shall be backed up and continuously, automatically updated. Only data that has changed since the last update shall be updated. The back-up server shall be separate from main server, preferably located a safe distance away.

6.7.3 Backup of card enrollment profiles and metadata

The storage capacity of a server must be up to 10 000 000 entries of access control card holders details and access control transactions. The data is permanently stored on the server until removed by the Systems Administrator. Metadata is excluded from this required capacity. Data on the storage shall be stored encrypted according to Transport Cryptography Standard.

6.7.2 Data Storage

RDBMS shall be fully ACID (Atomicity, Consistency, Isolation, Durability) compliant.

The database systems shall be based on relational database management system (RDBMS), fully supporting Structured Query Language, SQL:2011 standard or later. The SQL:2011 or the latest standard shall include full support for ISO/IEC 13249 SQL Multimedia and Application Packages or later.

6.7.1 Relational Database Management System

Relational Database Management System (RDBMS) with associated Application Programming Interface (API) shall provide server functions to the Access Control System.

6.7 Access Control System Server

- *Security*: AMS shall enable the following to be defined or set:
 - Authorized users
 - Passwords
 - Different user-access levels, for example;
 - * Administrator: access to all functionalities
 - * Operator: access to prescribed or defined functionality
 - Which authorized users have access to which components of the system and what actions can these users perform on the system.
- *Audit log files*: AMS shall provide audit log which presents a list of user actions based on user profile.

6.7.5 Archiving Server and Database Backup

If the Access Control Server reaches its storage capacity, it will automatically upload certain amount of data to the archiving server to open up space, using the principle of first in first out (FIFO). The targeted data is the access control card transactions.

7. Anti-virus software

All Operating Systems shall be installed with suitable and stable versions of anti-virus programs as per OS Developer specification and anti-virus software updates shall be installed as per OS developer recommendations. These installations shall be conducted once advice, recommendations and systems stability assurance have been received from OEM or OEM's accredited partner.

8. Patches Installation and Systems Updates

Operating Systems shall be patched according to OS Developer recommendations and specifications. These patches shall be installed once advice, recommendations and systems stability assurance have been received from OEM or OEM's accredited partner.

Systems software updates to enhance whatever vulnerability that is identified shall be carried out as per OEM's or OEM's accredited partner recommendations, without delay. Updates to the OS shall be conducted as per OS Developer or Distributor recommendations and in consultation with OEM or OEM's accredited partner.

9. Login Banners

Login banners shall be implemented as described in (Transnet Security Standard, 2014, p.9).

10. Vulnerability Scanning

Periodic scanning of all networked connected devices for vulnerabilities shall be conducted as described in (Transnet Security Standard, 2014, p.11).

11. Uninterrupted Power Supply (UPS) Units

- The UPS units shall comply with the requirements of SANS EN 50091. Each unit shall be able to handle all systems components connected to it in case of power outage, as per OEM specifications, to prevent data lost and data corruption.
- The entire UPS systems shall be controlled and managed by software management system integrated into the main system whose functions shall be;

- UPS configuration
- Checking UPS state, in particular battery status
- Setting and resetting of the unit
- In general full management of deployed UPS systems by a computer software

12. Control Rooms

The systems (Camera Surveillance and Access Control) shall be monitored and operated from the Control Room. All Control Rooms shall be built with solid walls in line with MISS standardization and be restricted areas with full access control and monitoring devices installed to control entry and exit. The size of each Control Room shall be determined by the size of the systems being monitored and the number of operators required per shift.

Abtution facilities, rest rooms and kitchens shall form part of a Control Room. Air-conditioning systems shall be provided for Control Rooms to ensure appropriate comfortable temperatures for Control Room users and adherence to OEM's specified operating temperatures for viewing stations.

13. Server Rooms

Server Rooms for surveillance and access control systems may be adjacent to Control Rooms or completely separately located. Their sizes and construction shall adhere to Transnet server room standards and Original Equipment Manufacturer (OEM)'s specifications.

The construction of Server Rooms shall adhere to MISS Control Room construction. All Server Rooms shall be well air-conditioned with industry standard air-conditioning systems satisfying OEM's specifications.

14. Enrollment Office

Each site with an Access Control system shall have an Enrollment Office well equipped with Access Control enrollment system, card testing equipment and well lit for excellent card photos.

Spare cards, computer consumables (printing ribbons, cartridges) shall also be kept in this office.

The Office shall be located in a convenient spot within the premises, easily accessible to card applicants.

15. Surge Protector

The entire security system must be protected against power surge, through the use of Surge Protector Modules(Units) or any industry standard power surge mechanism. In particular, surge protection mechanism shall ensure that;

- video is not lost, degraded or distorted, (Natcom, 2013) during power surge
- no equipment or device is damaged during a spike
- "if the surge protector module receives a hit beyond its capacity, the unit must "self-sacrifice" and protect the connected equipment from damage", (Natcom, 2013).

16. Integrated Systems

Integrated systems within Transnet shall be understood in the context of the following two complementary definitions: "In *engineering*, systems integration is defined as the process of bringing together components into one system and ensuring that the subsystems function together as a system. In *information technology*, systems integration is the process of linking together different computing systems and software applications physically or functionally, to act as coordinated whole.", (Wikipedia, 2014).

Within the context of the above definitions, camera surveillance, access control systems and related subsystems within Transnet shall be implemented and function as integrated systems or shall be integrated with integration platform.

17. Time Synchronization

Camera surveillance and Access Control systems and their related subsystems and network devices under their control that are time dependent shall be time synchronized by using Network Time Protocol (NTP) server, according to South African local time.

18. Intercom and Public Address Systems

Integrated to Surveillance and Access Control systems shall be the inter-communication (intercom) and Public Address (PA) systems.

The intercom shall allow two-way communication between the Access Control System users and the Control Room at the access control points. Intercom audio sound quality shall as described in "5.10 Audio".

Operators in the Control Room or anyone authorized and connected to the system shall be able to address users of the premises through the PA with stereo sound quality or with sound audio as described in "5.10 Audio".

18. Variable Message Signs

The system shall support writing and display of variable messages in the desired areas. The messages can be generated from the Control Room or anywhere in the systems network by an authorized person.

19. IP Ratings

All electrical appliances shall be IP66 (International Protection 66) or IP67 rated, depending on environment.

20. NEMA Ratings

For electrical enclosures, NEMA (National Electrical Manufacturers Association) rating NEMA 6P shall be met. NEMA 6P is equivalent to IP67.

21. IECx and ATEX Certifications

In some explosive environments, cameras and their housing shall comply with IECx (International Electrotechnical Commission) or ATEX (Atmospheres Explosives) specifications.

22. Documentation

Full systems documentation shall be kept and be updated periodically as described in (Transnet Network Security Standard, 2014, p.11). All network devices and their location shall be clearly indicated on a map drawn according to scale.

23. Firewall

All Transnet security systems shall be behind a firewall. Firewall installation, configuration, operation and management shall be as specified in Transnet Firewall Standard.

24. Adherence to OEM Specifications and Transnet Computer Hardware Standards

All hardware, software and systems operational framework shall be as per OEM specifications. All major hardware components, e.g. motherboards, CPU, memory and memory sizes, hard drives, graphics card, monitors used shall be 100% compliant to OEM specifications and comply with Transnet Computer Hardware Standard. The OS, architecture, applications programs, development toolkits and security programs used shall be as specified by the OEM and comply to Transnet Software Standard.

25. Systems Installation Standards

Vendor and OEM equipment installation standards, best practices and workmanship shall be applied to all equipment, network devices and cables that form part of the systems being installed. OEMs and vendors of repute have over the years developed their own guidelines and best practices based on empirical data and years of experience conducting field assessments and applying industry standards (Cisco Systems, 2014, p.1), to guide installers on how best to install respective (OEMs/vendors) technologies.

26. Violation of the Standard

All employees, third parties, contractors and other relevant individuals to which this standard applies shall comply with the requirements of the standard. Violation of any of the provisions of the standard without a formally approved deviation or waiver may result in but not limited to:

- Total or partial cancellation of the design (systems design);
- Cancellation of the contract with a service provider;

- Initiation of legal action by Transnet including, but not limited to, criminal or civil prosecution under applicable laws;
- Disciplinary sanctions against employees involved and/or implicated;
- Invocation of legal remedies such as those included in contractual agreements and Service Level Agreements including the cancellation of contracts with third parties and contractors.

References

- [1] Forouzan, B. A, *TCP/IP Protocol Suite*, McGraw-Hill, New York, 2010.
- [2] Natcom Group (PTY) LTD, *Integrated Electronic Security and Related Systems Specifications*, Pretoria, 2013
- [3] Nilsson, F, *Intelligent Network Video*, CRC Press, Boca Raton, 2009
- [4] EIMS, *Transnet Network standards*, Transnet, Johannesburg, 2014
- [5] EIMS, *Transnet Cryptography Standard*, Transnet, Johannesburg, 2014
- [6] *Systems integration*, (a wiki article), September 29, 2014, Available from http://en.wikipedia.org/wiki/System_integration, [26 November 2014].
- [7] EIMS, *Transnet Network Security Standard*, Transnet, Johannesburg, 2014
- [8] Cisco Systems, Inc., *Guidelines and Best Practices for the Installation and Maintenance of Data Networking Equipment*, Cisco Systems Inc., 2014