ABUAD Journal of Engineering Research and Development (AJERD)
ISSN (online): 2645-2685; ISSN (print): 2756-6811

Volume 4, Issue 1, 98-108

Integration of Public Surveillance System into Telecommunication Regulatory Framework in Nigeria

Abayomi Temitope AYODELE[1], Bayode Julius OLORUNFEMI[2], Sunday Emmanuel KAYODE[3], Ajayi Peter OSASONA[4]

[1]*Department of Mechatronics Engineering, Federal University Oye-Ekiti, Nigeria*
abayomi.ayodele@gmail.com

[2]*Department of Mechanical Engineering, Federal University Oye-Ekiti, Nigeria*
bayode.olorunfemi@fuoye.edu.ng

[3]*Department of Agricultural and Environmental Engineering, Federal University Technology, Akure, Nigeria*
kayodese01@gmail.com

[4]*Logistics and Supply (Works) Department, Nigerian Police, Force Headquarter, Abuja, Nigeria*
osasonajayi@gmail.com

Corresponding Author: bayode.olorunfemi@fuoye.edu.ng, +2348036061994

Date Submitted: 07/01/2019
Date Accepted: 30/11/2019
Date Published: 30/06/2021

Abstract: *The objective of this research is aimed at meeting the need for a well-managed and an adequately regulated, and legislation of specific area of Social Security system; the Surveillance system using Close Circuit Television (CCTV) in Nigeria. Interviews and questionnaire was adopted to obtain primary data to assess the degree of demand and yearning of average Nigerian. This process signifies adopting the process of Quality Function Deployment (QFD), which entails ensuring that a prospected deployment meets the yearning of the consumers or the stakeholders. The prospected legislation is tagged 'Inter-passages Surveillance and Un-coverage' Act (pronounced as 'I See You' Act.), to pass a message of notice of caution to everyone. The integration with Telecommunication Regulatory body will enhance quick and intelligent globalization of service and informed holistic structural implementation. This work would therefore be useful for government, corporate bodies, community, area, town, local area, States, and individuals on surveillance work, network, and management for an informed steer on her prospected formulation, regulation, and legislation of surveillance CCTV system.*

Keywords: *Closed-Circuit television, Public, Regulation, Security, Surveillance.*

1. INTRODUCTION

Public surveillance systems are comprised of a network of cameras and components for monitoring, recording, and transmitting video images. New systems typically incorporate cameras with good image quality; the ability to pan, tilt, and zoom; and capabilities such as color recording and night vision. Most cameras are pre-programmed to scan an area following a set pattern (referred to as a tour) and can also be operated remotely by security personnel or automated computer surveillance programs to focus in on specific areas or activities of interest. More sophisticated systems incorporate audio equipment or motion sensors that provide additional information about the monitored space, including detecting gunshots or recognizing license plates [1].

Surveillance system is aimed at improving the social security of any place and reducing the risk level of the place to bearable level and to the level that can be monitored [2] which could be termed as setting the risk to, as low as reasonably practicable [2]. Social security entails the uses public funds to provide a degree of economic security for the public [3]. Application of telecommunication systems and principles is becoming critically evolving, well stabilized in developed countries but gaining grounds in developing ones [4].

The whole essence of social security in this regards, is to cause deterrence against the perpetuation of evil so as not to destabilize the state of well being of an environment. The widespread frustration and deep sense of insecurity to life and property, occasioned by this epidemic, has become a matter of concern to government, security agencies, and the Nigerian citizenry at large [6]. The situation has become so critical, consequent upon the apparent helplessness of the law-enforcement agencies to stem the tide of the epidemic [3]. The state of insecurity in Nigeria today is such that the Nigeria Police Force do not even have adequate clue to solving the problems important.

The state of insecurity in Nigeria today is such that the Nigeria Police Force do not even have adequate clue to solving the problems, every of their very good intentions more or less places Nigerian nation under siege. The authority, in many instances, fails to turn adequate searchlight on the undercurrents of crime and violence and no adequate infrastructures, not minding that there are currently between 1,500 and 2,000 private security companies (PSCs) in Nigeria, employing in excess of 100,000 people [6]. Therefore, the use of mobile telecommunication handsets to monitor footages should be a welcome idea. UN indicates that 67 % of the world's population numbering 4.6 B are mobile subscribers as at 2009, the number continues to grow. The fourth generation 4G, true broadband wireless: WIMAX, 3G LTE, 802.11 a/b/g/n are the new technology that can efficiently deliver identifiable footage is already in place [7] & [8]. This is within the context of emerging rich media broadband wireless.

Video surveillance or closed-circuit television (CCTV) has become a highly popular and prevalent method of preventing crime in public space in many countries across the world. Although it often dominates the policy focus, questions have been raised about its effectiveness and social costs, as well as how it compares to alternative surveillance measures. A theoretical and programmatic understanding of surveillance draws attention to other widely used surveillance measures that perform a crime prevention function in public places. These include improved street lighting, security guards, place managers (e.g., bus drivers and parking lot attendants), and defensible space (i.e., changes to the built environment). This article reviews the research evidence on the effectiveness of the full range of public area surveillance measures and examines related social costs. It also serves to broaden the view of public area surveillance beyond the current narrow focus on CCTV.

1.1 Surveillance in the Context of Security in the Developed World

Surveillance can either be physical surveillance cyber surveillance or cameras, odour prints, radiation detection technology, radio frequency identification (rfid), smart video surveillance, eavesdropping, face-recognition and other biometrics, "no fly" and similar watch lists. all of these are different types of surveillance system.

Cameras have been used for decades to monitor traffic, to detect and prevent crime and to keep watch on private businesses and. As at 2005 in Britain, there are more than four million closed circuits Televisions (CCTV) cameras. Out of these are 1,800 cameras in railway stations; 6,000 in underground train network and buses while in the US, there more than 5,000 cameras in New York City's transportation systems while in the US Border Patrol uses Remote Video System ("RVS") along borders, costing over $64 million in the 2005 [9]. National Security Agency ("NSA") uses Echelon- global electronic eavesdropping system for Eavesdropping to bug telephone, e-*mail*, Internet upload, download communications transmitted by satellite, microwave tower, cable, Information from terrorist supercomputers. (This further established the importance of Telecommunication in adequate implementation of CCTV operations).

Eavesdropping software-defined radio, a wireless technology, makes cell phones and computers easier to bug and makes intercepting device compatible with networks. [10]. Face-recognition and other biometrics such as below-skin fingerprints (capture swirling patterns of capillaries), palm scanners, below-skin fingerprints (capture swirling patterns of capillaries), iris scanners, gait-recognition systems, Radiation detection technology that include customs and Border Protection (CBP) which employs radiation-detection technologies at official entry points, Highly sensitive personal radiation detectors, radiation portal monitors, Hand-held radiation isotope identifiers, etc.

Radio frequency Identification (RFID) [11] which are tiny computer chips use electromagnetic energy in the form of radio waves to track things from a distance, this are nick named "spy-chips". This travels through briefcases, wallets, walls, clothing, backpacks, and windows without obstruction, disorientation, or detection. RFID chips can also read and retain biometric information, such as fingerprints and photographs. RFID can exist as tag as "Passive" RFID tags, that is, it has no own internal power source or as an active or self-powered RFID tags with own battery. RFID has been embedded into many objects till date, examples are: worker uniforms, Employee and student ID badges, toll transponders, Animals (pets and livestock), warehouse crates and pallets, Gasoline cards [11], consumer products, library books, toll collection systems such as EZ-Pass, key-less remote systems for cars, key-less remote systems for garage door openers. Others are clothing, passports, ATM cards, vehicles, US postage stamps, paintings, beads, nails, wires, and cash. Verichip, a glass capsule is a form of RFID device containment injected into human flesh for ID and payment purposes. RFID will continue to gain more utilization as is also in use for several other things. Pharmaceutical manufacturers on prescription medications, banks to identify and profile customers who enter premises, governments to electronically frisk citizens at invisible checkpoints, citizens track in airports and border-crossing points, track mail track, etc., employ the use of RFID.

Smart Video Surveillance is another surveillance system that combines with behaviour-recognition software to do some couple of things such as 'Learn' what 'normal' behaviour is; identify unusual activity to read body languages, and so on, and could work in conjunction with other technology such as facial-recognition systems. Surveillance in the cyberspace otherwise referred to as privacy intrusions can also be in various forms. These are the likes of click stream data analysis, cookies, man-in-the-middle attacks (TCP hijacking), Pharming (hacker's redirection of Internet traffic from one Website to another), Phishing, Internet user receives e-mail appearing to be legitimate and from reputable company, asking user to reply with updated credit card information. Others are "puddle phishing", Spyware, Voice over Internet Protocols (VoIPs), Web bugs (tiny, invisible image or graphic embedded into HTML-formatted website or e-mail message to track users' activities, clickstream data analysis (logs of transactions recently performed on Internet computers), and so on.

Among the list are automated targeting system, automatic number plate recognition system, and communications assistance for law enforcement Act (CALEA) of 1994 CALEA petition for rule making, data mining, identity cards, biometric identity cards, and integrated automated fingerprint identification system.

Multi-state anti-terrorism information exchange (MATRIX) which is a web-enabled storage system to identify and combat criminal activity are as security recipes in developed countries. These include, though not limited to: Aircraft and other property ownership records, bankruptcy filings, corporate filings, criminal history records, digital photographs, driver's and pilot's licenses, state professional licenses, State sexual offenders' lists, terrorism watch lists, vehicle registrations, and soon. In the same manner, we also have: "secure flight" and other targeting systems, boarder patrol targeting systems enhancement, semantic information fusion, secure flight passenger-screening program, sharing/databases, terrorist screening database of the terrorist screening centre, and total information awareness (TIA) [12].

In United Kingdom, regulation of CCTV is not very well pronounced, however, British Information Commission issued 'Code of Practice', which dictates a framework on how the Data Protection Act should be implemented as regards to CCTV. This is nonetheless supported by several different other regulatory tools, which includes registration of systems, as it is the practice in France, Norway and Sweden, notification order for enhance transparency (Figure 1).

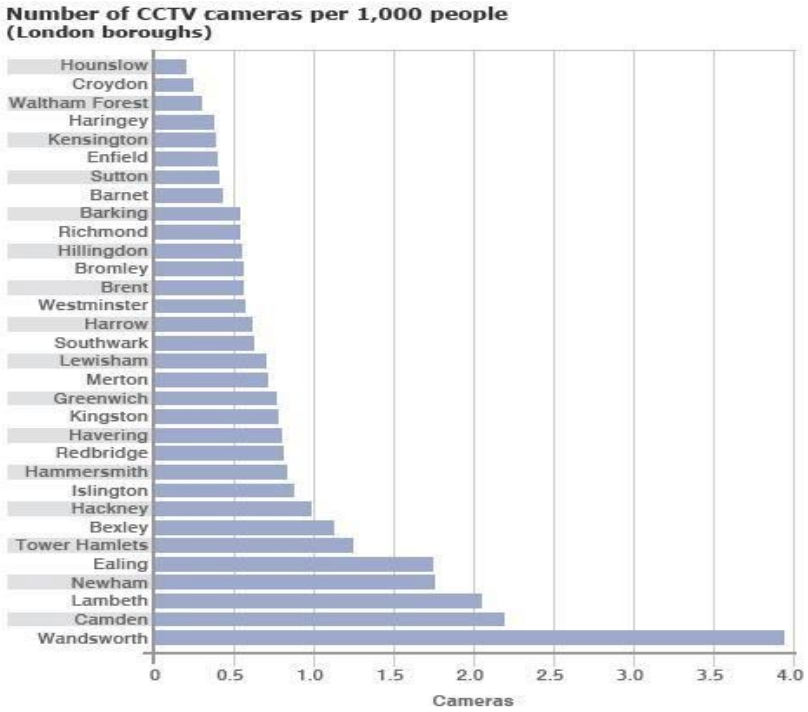


Figure 1: Number of CCTV cameras per 1000 people in United Kingdom [8]

All the aforementioned are indication that a national surveillance system which will adequately and effectively stem crime will look beyond mere installation of CCTVs but rather inculcate equally intelligent systems, organizational setups, legislation and regulations that is fear to all. Therefore, the earlier Nigeria established a well-legislated Act, adequately positioned structures and dedicated body within the telecommunication sector for CCTV implementation [12].

1.2 Surveillance System (CCTV) in the Context of Security in Developing Countries

The transfer of surveillance systems to developing countries can aid national security, or risk becoming technologies of political control [13]. Hence, solution to national security with surveillance systems such as CCTV only is not the solution but bringing it on with qualitative and effective regulations and legislation. For developed countries, the instituted Acts in this regards is delivered with intelligence surveillance systems to enforce the laws. Nevertheless, the misuse of surveillance systems has necessitated putting in place adequate legislation, otherwise, there will be abuse of different dimensions, this is an advice given by Griffith [15] in his book titled 'Caribbean Security on the eve of the 21st Century'. Figure 2 is an example of CCTV public camera while Figure 3 shows a monitoring studio.

1.3 ITU and CCTV

International telecommunication Union (ITU) maintains a summed stance on the requirements and service description for visual surveillance by the way of standards. These include SERIES F: Non-telephone telecommunication services F.743 tagged 'Draft new ITU-T Rec.' F.743 (ex F.VS-reqs) which describes the visual surveillance system framework, service scenarios and specific service requirements that pertain to visual surveillance [16, 17].

Real-time surveillance, recording and alarming, convergence of visual surveillance and other services such as sensor networks, multimedia conference, IPTV service, etc. Requirements for Visual surveillance at the level of User level

requirement, basic requirements, advance requirement, so do for service requirements, security requirement with recommendation on authentication, access, content, system security and network security, network and control requirement, quality of service, quality of experience and management requirements.

Figure 2: Public surveillance CCTV camera

Figure 3: Monitoring studio

2. MATERIALS AND METHODS

The methodology [19] applied in the research entails sample selection, bench marking, data gathering through questionnaires and data analysis methods (qualitative and quantitative). Consultations were made with ranges of stakeholders. Appendix 2 shows a copy of questionnaire drawn to capture information on security situation in Nigeria.

2.1 Design Consideration for CCTV

Many factors are required for the designing of CCTV network or systems. On the component level, quality of service or design performances will depend on the choices made on: cameras, lenses, monitors, video switchers, video multiplexers, video recorders, hard copy printers, ancillary equipment and video, power supply (critical in nigeria scenario) and transmission medium.

2.2 Design on Philosophy of Installation

On system level, it is appropriate to consider the Location where CCTV will be installed, the objectives of the installation, the coverage area, thus the number of CCTV camera required, the power requirement, Power supply consideration & management. It has to be ascertained that installation is such that can be powered 100% of the time, hence CCTV that has capability for efficient power management should be considered. The design should also consider the availability of power supply redundancy to enhance availability and power system protection to enhance safety. Source of power in Nigeria scenario could be from the National grid, or via Solar panels, (this will be okay for remote installation).

2.3 Design with Scheduled Maintenance Scheme

To sustain the integrity of any installation, maintenance scheme must always be put in place. This is a great leaning from the Great Britain system, which has a fantastic maintenance culture. Example of an adoptable CCTV Maintenance Checklist is to includes, history of CCTV system since last maintenance service, satisfactory transmission of images to remote centre, and repair faults where necessary.

2.4 Design with consideration analysis of risk of deployment in place

While implementing CCTV installation, risk analyses need to be conducted in relation to the environment, the set-up of the location of installation, for example, type of company, type of residence, the headroom, the assesses, traffics history and reports, and the infrastructure around the area such as Petrol stations, Power lines. Consideration should also be given to human behaviour, etc.

2.5 Design with Contractor Performance Tagging

This is achievable in two ways, first by putting in place pre-commissioning installation checklist before installation execution, every deployed system as a document for owner to compare with proposed design and diagram of deployment of system. This will ensure correct installation of each and all the component. Secondly, installer/vendor should be at all times be attributed with a 'performance tag' upon which decision to the selection of vendor or installer for subsequent deployment could be informed.

2.6 Standardizing System Management

On every installation and system deployed, there shall be the attestation of a representative of a Government regulator who will give a clearance certificate (CC). This certificate shall validate system deployed. The validation among other considerations shall be that the installation and integration are;

- Executed to standards (BS 7992, BS 4737 or BS EN 50131-1) [21] & [22] and
- Documentations abide by TQM [23].

3. RESULTS AND DISCUSSION

Data generated from the questionnaire distributed are presented pictorially in Figure 4 graphical interpretation of all the analysis above. 'No accepted' indicates the distribution of people that disagreed with the concept of deploying Surveillance system in Nigeria with other aligning factors considered. while 'Accepted' indicates the distribution of people that agreed with the concept of deploying Surveillance system in Nigeria with other aligning factors considered.

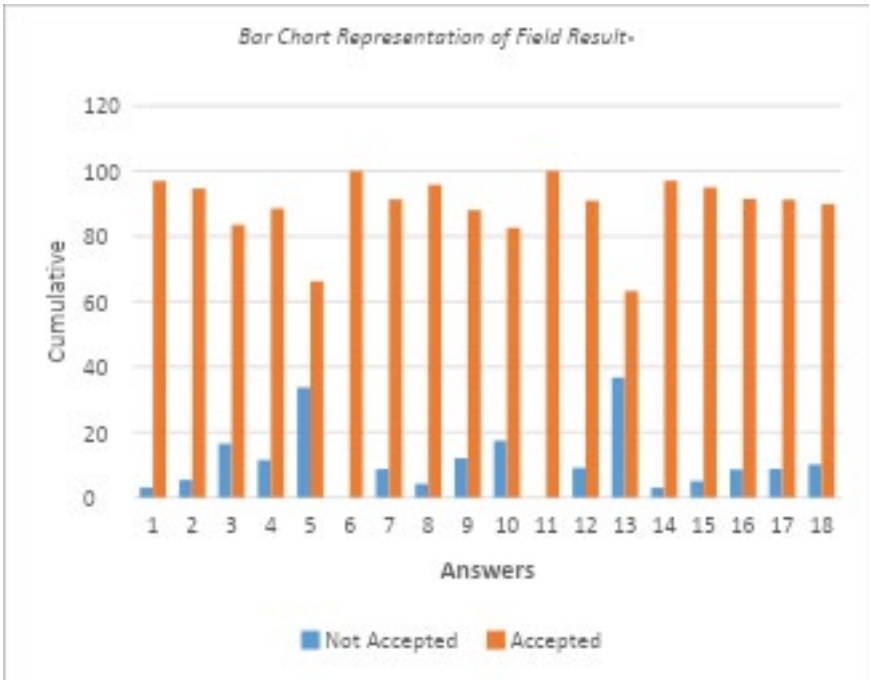


Figure 4: Bar chart representation of field results

The organization framework involved the strategies considered to be necessary for the implementation processes for ensuring the best practice Integration of Surveillance system into telecommunication framework in Nigeria. An interactive matrix and hierarchical network and HR organizational topology designed will be appropriate. The matrix content allows for backup or protection for better reliability. Figure 5 was the components of surveillance system developed.

3.1 Network Administrative Structure

For effective management of the surveillance network hierarchy chain, Table 1 shows the operation centre Identification Tags. Hierarchy identifier was set for each centre or operation hub, which will represent an identifier for the category of the operation centre from which information is transmitted. The National Privacy Commission (NPC) Headquarters office for example would have 10 as its identifier. Footage emanating from such centre shall have 10 at the start of its identifier

tag. The identifier tags represent remote location identifiers transmitting signal into a hub centre or a local concentrator. For instance, a tag 10.2 002.3 045.4 024.11 02, instance can be interpreted as;

- 10-traffic collection at NPC headquarters
- 2 002-From Territory tagged 2
- 3 045 emanating from Region tagged 45
- 4 024-State tagged 24.
- 11 001- and ad-hoc tagged 01.

A, B, C... K is tag numbers with a maximum Word Length of 4

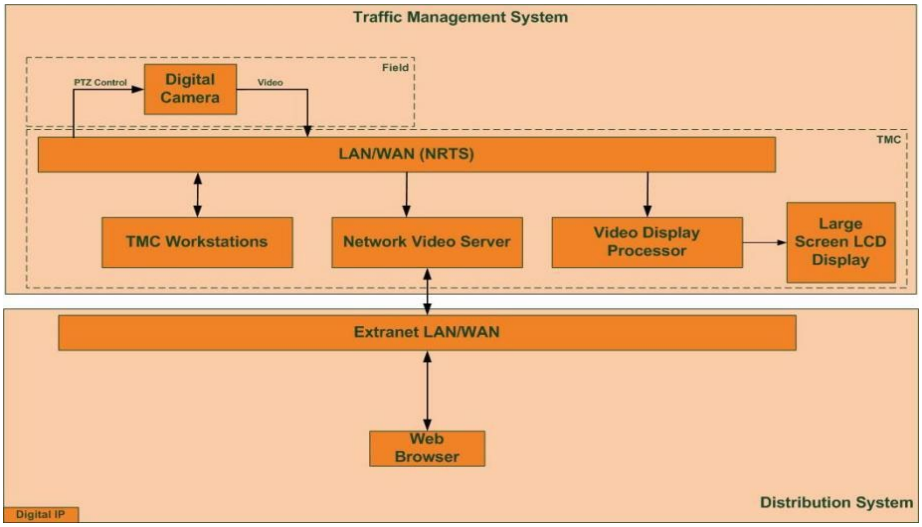


Figure 5: Components of 3G CCTV surveillance system

Table 1: Representation of operation centre identification tag

Name	Identification tag	Representation.	
National Privacy Commission (NPC) Hub centre.	10	10ABCD	10-NPC identifier
Territorial Surveillance Centre (TSC):	2	2A	2-TSC identifier
Regional Surveillance Centres (RSC):	3	3B	3- RSC identifier
State Surveillance Centres (SSC):	4	4C(EFG)	4-SSC identify
Senatorial Surveillance Operations (SSO):	5	5E	5 -SSO Identifier.
Primary Surveillance Centre (PSC)	6	6F(GHJ)	6- PSU identifier,
Area Surveillance Operations (ASO):	7	7G	7- ASO identifier,
District unit (DU):	8	8H	8- DU identifier,
Private Terminal Unit (PTU):	9	9J	9-PTU identifier
Ad hoc Surveillance Centres	2	11D	11-ASC identifier

Sample of specification Log Sheet for CCTV camera is shown in Figure 6. While a diagram showing their presentation of CCTV network system is shown in appendix 1. Results of Questionnaire for field assessments presented in Table 2.

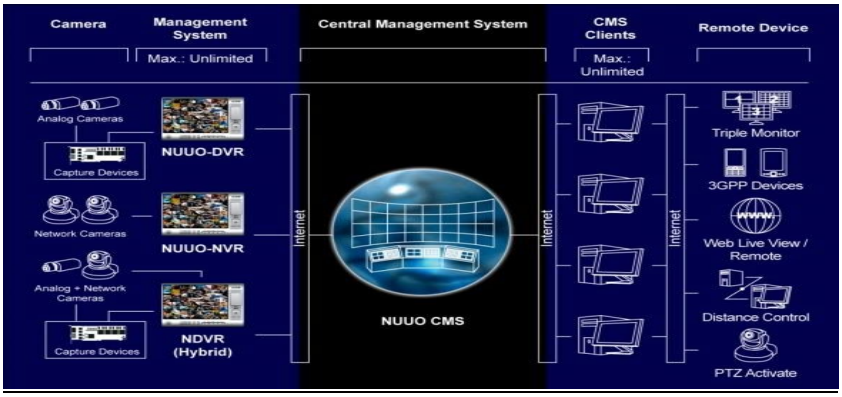


Figure 6: Sample of Specification Log Sheet for CCTV camera

Table 2: Table of field assessment and Questionnaire by Intrapolation

Camera No.	Position	Mount	Type	Colour/Mono	Lens	Angle	Coverage Required

CCTV OPERATIONAL REQUIREMENT CAMERA CHECKLIST				
Place/Premises				
Date		Sheet No		
Location.				
Objective of installation.				
Likelihood of an activity occurring	High	Frequency of activity occurring	Regularly	
	Medium		Often	
	Low		Occasionally	
Purpose of Camera/ Quality of Picture Threshold	Recognition		Identification	
Activity Lighting conditions.	Natural	Artificial	Night	All Conditions
Required camera operations	Zoom	Pan	Tilt	Other
(Tick/Note required special features)	Movement following	Tamper proofing		

3.2 Legislation (Human Right Act 1998)

This affects all the activities of Public-Authority relationships on the presentation of images. This Act dictates in using CCTV camera, five tests must be conducted:

- CCTV should not be used as an instrument of entrapment. German law, for example requires a justification and legislative basis for interference with an individual's right, except for authorized covert surveillance by police or other authorized government agents.
- Proportionality, that is, it has to be determined if CCTV [14] is appropriate and that will the quality be good enough for the solution sought?
- Legality, that is, will it be lawful to use CCTV?
- Accountability, saying that, are you following legislated direction on activities and,
- Subsidiarity, is the required minimum interference threshold with right understood and observed?

3.3 Data Protection Act (DPA) 1998

Data Protection Act (DPA) 1998 analyzed the processing of images from CCTV and it demands that:

- A user must ensure that the use for CCTV is fit for purpose,
- Comply with the DPA Code for CCTV and data processing
- CCTV activities should be manned by trained personnel,
- Ensure to register with the Office of National,
- Privacy Commission (in Nigeria).

3.4 Investigatory Power Act 2000

This is invoked specifically for covert activities for investigation purposes. This requires that the responsible entity will need to seek authorization before conducting covert surveillance.

At every level of surveillance 'Centre' operation, an agreement will be entered into, with private owners dictating service level agreement, outline of roles each stakeholder, responsibilities and liabilities across a range of issues including buildings, insurance, finance, staffing, system development and review. Specifically, for private operators or for individuals, a well-regulated system shall be in place, which will require a kind of licensing system. All potential CCTV users including:

- Those who wish to use cameras to observe a 'protected object';
- Those who wish to improve a driver's sight when installed onto a vehicle;
- The national road union or authorities who wish to use it to observe traffic flows;
- Those who wish to observe weather conditions;
- Police keeping surveillance of a particular location for a short period, like 35 days for a grounded suspicion that a particular serious crime or incident will take place at a particular location.

The content of application shall include but not limited to the following:

- Detailed information about the applicant,
- An attached Criminal record /Police report of the applicant.
- Evidence of payment of Tax for 3 months with the last three months or working status to show clean record of no tax defrauds record.
- Clear information about the planned system and surveillance area;
- Third part agreement to surveillance if required (this shall be determined by the NPC);
- Acceptance to: inform of the surveillance by signposting in a conspicuous location, outside of the surveillance area.

Base on the application and demographic analysis, an application can be granted in part or as a whole or be rejected, for a limited time or for the period applied.

3.5 Standard for References

This part will rely majorly on ITU-T F.743. Other standards relied upon in this framework are as follows:

700] ITU-T Recommendation F.700 (2000), Framework Recommendation for multimedia services.
701] ITU-T Recommendation F.701 (2000), Guideline Recommendation for identifying multimedia service requirements.
702] ITU-T Recommandation F.702 (1996), MultiMedia conférence services [29].

3.6 Enforcement of Legislation

The legislation will have a duty of law to define Procedure for Consequence Management. Falsification of any kind or presentation of harmful document within this premise shall carry a conviction at a High Court with maximum penalty of, say one-year imprisonment and/or a fine up to N50, 000.00

3.7 Vicarious Liability Clause

There shall exist the clause 'Vicarious liability in the Act, this means that responsibility for acts committed by people in the course of their work is passed up to their employer. So in effect, not only is the person who acted indiscriminately be held accountable, but also the organization for which they work.

4. CONCLUSION

This work has identified the demand for surveillance system to drive an aspect of social security (Surveillance CCTV) in Nigeria. It has determined the way to implement the deployment, bench marking from other experience, however putting into consideration the demographic values of Nigeria as peculiarity.

With the appreciation of the values of a reliable system and organizational built-up, the research considers a CCTV network with a back pane of telecommunication infrastructure network and a protective system design to cover-up for either system or operational failure. To enable high availability, it considers a National Privacy Commission operating as an auspice of Nigeria Communication Commission (prospected the elevation of such to Nigeria National Communication Authority). The Analysis presented shows that Nigeria will benefit immensely in operating a Regulated and a Legislated Surveillance CCTV system deployment, which will stem societal security menace by its virtues of capability for deterrence and the effectiveness of the deployment, will be enhanced if integrated with Telecommunication system in the Country.

ACKNOWLEDGEMENT

The authors acknowledge the contributions of members, Faculty of Design Media and Management of Buckinghamshire New University, **United** Kingdom and Nigeria Telecommunication commission.

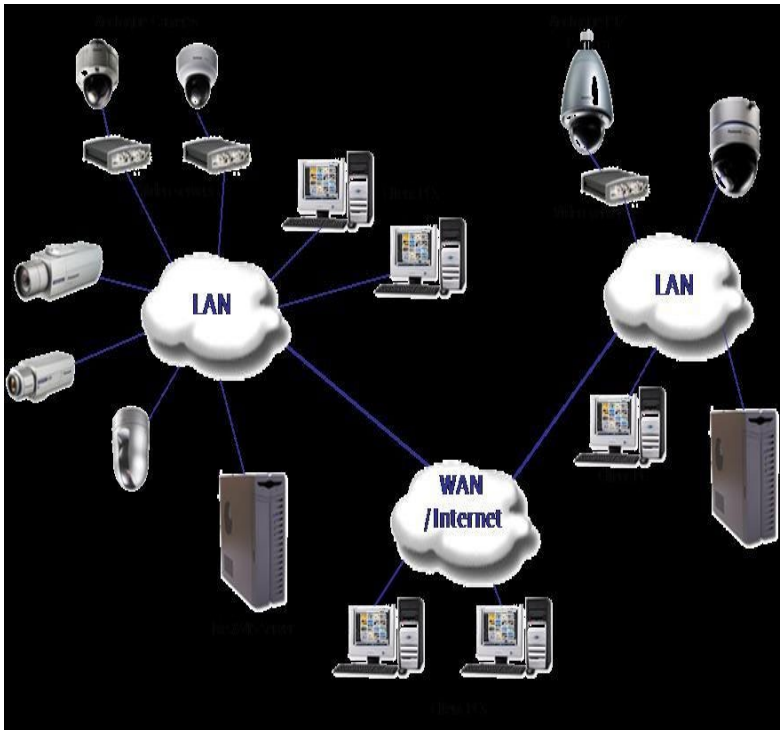
REFERENCES

[1] Surette, Ray. (2005). The Thinking Eye: Pros and Cons of Second Generation CCTV Surveillance Systems. Policing: An *International Journal of Police Strategies and Management*, 28 (1), 152-173.
[2] Martin Gill & Angela Spriggs, (2005) Assessing the impact of CCTV. Home Office Research, Development and Statistics Directorate, February.

[3] How Social Security Numbers Workhttp://people.howstuffworks.com/social-security-number1.htm. Web assessed 12/05/2019.
[4] Aldridge J., & Gilbert C., (1996) Performance Testing of CCTV Perimeter Surveillance Systems (Using the Rotakin Standard Test Target) Version 1.0. UK *Police Scientific Development Branch Publication* No. 14(95)
[5] Iziguzo, S. (2007), How We Robbed Redemption Camp. The Nation. . p.5 . Available: http://www.thenationonline.com
[6] Corporate Affairs Commission, Nigeria. 600,000 Companies registered so far. (Online) Available: http://allafrica.com/stories/200808041472.html web assessed 11/05/201
[7] CCTV Guide [Online] (2017). Available: http://www.iviewcameras.co.uk/pdf/cctv_buying_guide.pdf web assessed 12/05/2017.
[8] Vision Techniques fights anti-social behaviour with mobile CCTV vehicle security systems, http://www.vision-techniques.com/latest-news/vision-techniques-fights-anti-social-behaviour, web assessed 05/08/2018.
[9] Council looks at talking CCTV to curb anti-social behaviour, http://www.wavestore.com/security-cctv-news/council-looks-at-talking-cctv-to-curb-anti-social-behaviour/871/web assessed12/03/2011.
[10] Jeffrey Aresty, President, Internetbar.org, [Online]. Available:. http://www.cyberspaceattorney.com, Assessed on 14/11/2019
[11] University of Reading CCTV research praised by Home office. Available: http://www.info4security.com/story.asp?sectioncode=10&storycode-4124359 web assessed 05/05/2011
[12] Gina Marie Stevens (2003). American law division privacy: total information awareness programs and related information access, collection, and protection laws
[13] Video over 10G ip, The Siemon Company, http://www.siemon.com(2003). The Siemon Company WP-CCTV Rev. A 10/03. web assessed 26/12/2010.
[14] National Security and Surveillance in Developing countries. Available: http://www.suite101.com/profile.cfm/RichardEscalanteweb assessed 20/07/2017.
[15] Ivelaw Griffith (1996). Caribbean Security on the Eve of the Century. Institute of National strategic studies, National Defence University, Washington, DC.
[16] ITU-T Recommendations, http://www.itu.int/en/ITU-T/publications/Pages/recs.aspx, web assessed 10/05/2018.
[17] WallaceE., & Diffley C. (1998). CCTV: Making it work CCTV Control Room Ergonomics, UK Police Scientific Development Branch Publication no 14/98., 1-15.
[18] Privacy International Statement on CCTV Surveillance. Available: https://%20www.privacyintenational.org/%20%20article/privacy-international-statement-cctv-surveillance. web assessed 05/05/2011.
[19] Catherine Dawson (2002). Practical Research Methods, a user-guide to mastering, research techniques and projects. pages 1-139.
[20] Airport's Security Compromised by Misplaced CCTV Cameras and Empty Observation Towers http://beirutspring.com/blog/2010/07/13/airportssecurity-compromised-by-misplaced-CCTV-cameras-and-empty-observation-towers, web assessed 25/10/2011.
[21] Systems/Monitors/Cameras/Installations/Remote monitoring and Detector Activated (2006).Code of practice [BS8418], http://bs8418.co.uk/.
[22] Maintain operational performance of CCTV systems (draft) [Online] Available:, http://www.parkmark.co.uk., web assessed25/04/2011.
[23] Total Quality Management (TQM).http://www.businessballs.com/total_quality_ management_TQM.pdf, web assessed 25/04/2019
[24] Fatima Naseem, Training Slide, Wireless Communications, University of Engineering and Technology, Tesilaweb. Uettaxila.edu.pk/CMS/AUT2010/cpWCbs/notes% lecture.

APPENDICES

Appendix 1: Representation CCTV Network system diagram


LAN
LAN
WAN
/Internet

Appendix 2

QUESTIONNAIRE

Security System in Nigeria.

Please answer the following questions. Your inputs will only be used for research purposes, we will not in any circumstance refer to your personal identity as regards this questionnaire. Thank you for your cooperations.

1.1 I am a Nigerian :

Yes		No	

1.2 My Gender is :

Male		Female	

2 Please use the keys table 2.1 to answer the questions in table 2.2 below .

Table 2.1.

GRADES :	Critically Accepted	Accepted	Neutra	Not Accepted	Critically not Accepted
Key	5	4	3	2	**1**

Table 2.2

	Question	**Answer**
Example 1	*There 24 hours in one day*	*5*
Example 2	*10 days makes a week*	*1*
1	Security is a **major problem** in Nigeria	
2	Nigeria Police are **NOT** doing very well to curb security problems in Nigeria.	
3	Nigeria Police contributes to Security **vices** in Nigeria.	
4	Government has **NO** effective policy on human security in Nigeria.	
5	One of the reasons why you do not frequently visit Nigeria is because of the insecurity in the country.	
6	The security status of Nigeria affects business and drives investors away.	
7	Many Nigeria intellectuals run away from, and out of Nigeria because of her security status.	
8	Security impetuses in Nigeria are not functioning well.	
9	There is need for a new functional legal frame work for security in Nigeria.	
10	Installation of Personal communications systems or services (e.g. using CCTVs and mobility system) will help on security status in Nigeria.	
11	Government needs to create a functional Legal Frame Work for the operation and monitoring of CCTV and liberalize it such that anyone can view life CCTV footage at anytime and from anywhere.	
12	Government to set up a New and Credible Agency to Drive the new surveillance security system.	
13	Everybody to be able to assess overt CCTVs on any Mobile set.	
14	Nigeria needs improved security status to foster development of the country.	
15	Government to partner with private sectors and individuals to ensure installations of necessary surveillance systems to curb security problems in Nigeria.	
16	Nigeria Government to declare a state of emergency on the present security status of the country.	
17	You are willing to contribute your own quota to the success of improving the security status of Nigeria if required.	

Please write your other personal comments or information here:

Thank you.