

DJR3B - SECURITY MANAGEMENT, PRIVATE DETECTIVE AND INVESTIGATION

Unit I Security

Security: Ancient Period, Anglo-saxon period; The American and British Development. Developments in India - Role of CISF in Industrial security, Security Areas: Exclusion Area, Limited Area and Control Area. Physical Security Barriers: Natural Barriers, Structural Barriers, Human Barriers, Animal Barriers

Unit II Duties of Security Staff

Duties of Security Staff: Chief Security Officer, Security Officer, Security supervisor and Security guards.

Unit III Security Systems

Interrogation, Investigation and taking of statements - Liaison with local police-employees participation in Industrial security — Use of Dogs in Industrial Security.

Unit IV Surveillance

Surveillance: Purpose, Pre-surveillance Conference, Covert and overt Surveillance, Automobile Surveillance, Foot Surveillance, Team Surveillance

Unit V Types of Investigation

Pre and Post Marital Investigation – Land Dispute investigation - Student Investigation, Kidnapping and abduction investigation – missing person investigation – Traffic accident investigation Pre-employment verification, Post employee.

UNIT-I: SECURITY

Introduction

The term 'security' connotes to wide range of ideas in our daily walks of life. Security does not talk about the individual or a group of people or a place, Security deals with the society at large. In brief, the term 'security' can be defined in simple terminology as to "Safeguard and protect the people, place, property, and assets from the hands of evil and criminal and anti-social elements in the society. If we go thoroughly with the pages of history, we find adoption of various methods of security measures to secure their life, land and property from the intruders or invaders in the past and present, In the present era of technological development the term "Security" has taken a different shape we have seen a wide range of modern technology to assist us in adopting the security measures to prevent from loss, theft and burglary in our modern times. We can also see the modern sophisticated devices which monitor each friction of moment in a computerized system to safeguard the life, property and prevent the crime in the society.

The concept of security can be traced back to ancient period of Stone age, where in the cave man Cavemen originally used rocks, fruit, branches, and other natural resources to ward off predators and keep themselves out of harm's. Over the centuries and decades, the concept of security has taken the form of playing a significant role in the modern-day society in a wide spread manner. The most elaborate security system during the ancient period was the great wall of China, built 20 years ago by emperor Chin to guard China from Mongols, requiring 15 years and half a million laborers to build, the wall was long enough to stretch from New York to Mexico. Rome also emphasized and designed to form a physical security and patrolling by legions and bridges controlled by iron gates and guards. However, rules went beyond control and there came the requirement of deploying the armed guards to enhance the security over the region during the ancient period, in the recent trend the industrial security plays a pivotal role in the modern-day life, Industrial security is to maintain a state of being secure from the threats and danger for the 4Ms viz. Men, Material, Machinery and Money. In some sectors security is also know by the term "Watch & Ward".

The Anglo- Saxon period in England (A.D 500- 1066) is significant because its customs of protections are still applied today. This was the time when Romans were unable to conquer England. Security and law enforcement were a community responsibility. When a Crime occurred, “hue and cry” was sounded as a community banded together to capture the offender who has committed that crime, in today era we have citizen arrest and *posse comitatus* (i.e an authority requesting citizens to assist with stopping unlawful behavior).

The concept of security emerged between United States and British during the aftermath of WW II initially focusing on the strengthening the Military strength between the countries it now encompasses a broad range of facets, all of which impinge on the non-military or economic security of the nation and the values espoused by the national society. During the Bilateral talks between the countries the following measures were taken to ensure the National Security

- Using diplomacy to rally allies and isolate threats.
- Marshalling economic power to facilitate or compel cooperation.
- Maintaining effective armed forces.
- Implementing Civil Defense and emergency preparedness measures including anti-terrorism legislations.
- Using Intelligence Services to detect and defeat or avoid threats.
- Using Counter Intelligence services or Secret police the nation from internal threats

Role of CISF (Central Industrial Security Force)

The Central Industrial Security Force (CISF) (established in its present form: 15 June 1983) is a Central Armed Police Force in India. It was set up under an Act of the Parliament of India on 10 March 1969 with a strength of 2,800. CISF was subsequently made an armed force of the Republic of India by another Act of Parliament passed on 15 June 1983. Its current active strength is 144,418 personnel, In April 2017, the government raised the sanctioned strength from 145,000 to 180,000 personnel. It is directly under the Union Ministry of Home Affairs and its headquarters are at New Delhi.

The CISF provides security cover to 300 industrial units, government infrastructure projects and facilities and establishments located all over India. Industrial sectors like atomic power plants, space installations, mints, oil fields and refineries, major ports, heavy engineering, steel plants, barrages, fertilizer units, airports and hydroelectric/thermal power plants owned and controlled by Central Public-Sector Undertakings (PSUs), and currency note presses producing Indian currency are protected by CISF. It thereby covers installations all over India straddling a variety of terrain and climatic conditions. CISF also provides consultancy services to private industries as well as other organizations within the Indian government. The consulting wing has amongst its clients some of the renowned business houses and organizations of India including TISCO, Jamshedpur; SEBI Hqrs. Mumbai; Vidhana Sabha, Bangalore; Orissa Mining Co., Bhubaneswar; Telangana Assembly, Hyderabad; Bangalore Metropolitan Transport Corp.; HIL Kerala; IB Thermal plant, Odisha; IARI, Delhi; NBRI, Lucknow and Electronics City, Bangalore. The scope of CISF's consulting practice includes security consulting and fire protection consulting.

CISF is just a unique organization in paramilitary forces for India, which works for sea ways, airways and some of the major installations in India. In CISF there are some reserved battalions which works with the state police to protect law and orders. CISF plays a major role in Disaster Management, for Disaster Management course the personnel are trained from NISA, Hyderabad. Another unique thing which the CISF has is a Fire Wing which helps during fire accidents in Industries where CISF is on guard.

However the role of CISF has undergone a diversification in the recent period after the raise of security threats in the country the government has brought in measures where in CISF is deployed in high security and sensitive areas to guard and protect, therefore it now protects airports, seaports metro rails seaports, metro rail networks, government buildings, heritage monuments (including the Taj Mahal and Red Fort), opium and alkaloids extractions, nuclear power plants, and space installations. It also specializes in VIP, VVIP and Z category security as well as disaster management.

Security areas:

The security design mainly operates on the topology of the area and it varies geographically from place to place, when the security design is drafted or implemented, the below mentioned areas are taken into consideration before the roll out process of security.

Exclusion area:

An exclusion zone is an area where people are not allowed to go or where they are not allowed to do a specific thing, for example because it would be dangerous. The Exclusion area can be otherwise called as Restricted area, this installation or activity has been declared as restricted area by an Authority of (Title, COMMANDING GENERAL OR COMMANDING OFFICER) in accordance with the provision of the directive issued by the secretary of the defense on 20 August 1954 in accordance to the law provision of Sec 21, internal security act of 1950 and unauthorized entry is prohibited.

All persons and vehicles entering herby are liable to search. Photography or making notes, drawing maps are graphics representatives of this area or its activities are prohibited unless specifically authorized by the commander. Any such material found in the possession will be confiscated.

Limited area and Controlled area:

A controlled area is defined as a room, office, building or other form of facility to which access is monitored, limited, or controlled by either physical guarding or electronic guarding of the location. Admittance to a controlled area is limited to persons who have official business within the area. Responsible managers are authorized to designate an area as a controlled area after adequate security measures are in place. The following areas should be designated as controlled areas:

- (1) An area where classified information or highly sensitive information is handled, processed, or stored. A mailroom is considered such an area.
- (2) An area that houses equipment that is significantly valuable or critical to the continued operations or provision of services.

- (3) An area where uncontrolled access would interfere with or disrupt personnel assigned to the area in carrying out their official duties.
- (4) An area where equipment or operations constitute a potential safety hazard.
- (5) An area that is particularly sensitive as determined by the responsible manager.

Physical Security barriers:

Physical security barriers are the foundation layer of any organization that has a robust security operations, Physical security barriers are structural barriers that are man-made devices such as fences, walls, floors, roofs, grills, bars, or other structures that deter penetration and also at the same time the physical guarding of the location by the man guarding plays a significant role . There are different kinds of barriers apart from the man guarding each ones are elaborated as follows

Natural Barriers:

Natural barriers are the barriers that are not man made and nature has formed on its own to prevent the invasion or intrusion of any foreign objects into the territory include mountains, cliffs, canyons, rivers, or other terrain difficult to traverse Mountains, swamps, deserts and icefields are among the clearest examples of natural barriers. Rivers are a more ambiguous example, as they may obstruct large-scale movement across them (especially by armies) but may facilitate smaller-scale movement along them in boats, once some of the people in the region have developed the relevant technologies. Seas have likewise been an obstacle at first, then a convenient medium for transport along coastlines, and finally a medium for intercontinental transport. Natural barriers have been important factors in human history, by obstructing migration and invasion. For example, Jared Diamond argues that West European nations have been the dominant powers of the last 500 years because Europe's many natural barriers divided it into competing nation-states and this competition forced the European nations to encourage innovation and avoid technological stagnation.

Some examples of natural barriers are the Himalayas isolating Indian subcontinent from the rest of Asia, the Grand Canyon, the Dead sea, and the Mississippi river.

Structural Barriers:

Structural barriers are man-made devices such as fences, walls, floors, roofs, grills, bars, or other structures that deter penetration. If a natural barrier forms one side or any part of the perimeter, it should not automatically be considered an adequate perimeter barrier, since it may be overcome by a determined intruder. Structural barriers should be provided for that portion of the perimeter, if required in an organization based on the risk assessment conducted as per the topography of the location where the organization is situated.

Fencing:

Fences are the most common perimeter barrier or control. Two types normally used are chain link and barbed wire. The choice is dependent primarily upon the degree of permanence of the facility and local ordinances. A perimeter fence should be continuous, be kept free of plant growth, and be maintained in good condition.

Chain Link:

Chain link fencing should be laid out in straight lines to permit unhampered observation. It should be constructed of number 11 gauge or heavier wire mesh (two-inch square) and should be not less than seven feet high and have a top guard. It should extend to within two inches of firm ground. It should be taut and securely fastened to rigid metal posts set in concrete. Anti-erosion measures like surface priming may be necessary. Where the fence traverse's culverts, troughs, or other openings larger than 96 square inches in area, the openings should be protected by fencing, iron grills, or other barriers to prevent passage of intruders. Chain link fencing is low in maintenance cost, a minimal safety hazard, and has openings small enough to discourage the passage of pilfered articles.

Barbed Wire:

Standard barbed wire is twisted, double strand, number 12-gauge wire, with four-point barbs spaced four inches apart. Barbed wire fencing, including gates intended to prevent trespassing, should be no less than seven feet in height plus a top guard, tightly stretched, and should be firmly affixed to posts not more than six feet apart. Distances between strands should not exceed six inches.

Top Guard:

A top guard is an overhang of barbed wire along the top of a fence, facing outward and upward at an angle of 45 degrees. Three or four strands of barbed wire spaced six inches apart are used, but the length of the supporting arms and the number of strands can be increased when required. The supporting arms should be affixed to the top of the fence posts and be of sufficient height to increase the overall height of the fence at least one foot. Where a building of less than three stories is used to form a part of the perimeter, a top guard should be used along the outside wall to deter access to the roof.

Gates:

The purpose of a gate is to provide a break in a perimeter fence or wall to allow entry. Gates are protected by locks, intermittent guard patrols, fixed guard posts, contact alarms, CCTV, or a combination of these. The number of gates and perimeter entrances should be limited to those necessary, but should be sufficient to accommodate the peak flow of pedestrian and vehicular traffic. Gates should be adequately lighted. They should be locked when not manned and periodically inspected by a roving guard force. Utility openings in a fence that do not serve as gates should be locked, guarded, or otherwise protected. Intrusion detection devices may be desirable when the gate is used intermittently or when a higher level of protection is desired. Alternatives to detection devices include coded card keys, push button combination locks, and CCTV.

Protective Lighting:

Protective lighting is a valuable and inexpensive deterrent to crime. It improves visibility for checking badges and people at entrances, inspecting vehicles, preventing illegal entry, and detecting intruders both outside and inside buildings and grounds. Locate protective lighting where it will illuminate shadowed areas and be directed at probable routes of intrusion. Also, overlap lighting to prevent dark areas. If justified, include emergency power for lighting.

Doors:

A door is a vulnerable point of the security of any building. A door should be installed so the hinges are on the inside to preclude removal of the screws or the use of chisels or cutting devices. Pins in exterior hinges should be welded, flanged, or otherwise secured, or hinge dowels should be used to preclude the door's removal. The door should be metal or solid wood. Remember that locks, doors, doorframes, and accessory builder's hardware are inseparable when evaluating barrier value. Do not put a sturdy lock on a weak door. The best door is of little value if there are exposed removable hinge pins, breakable vision panels, or other weaknesses that would allow entry. Transoms should be sealed permanently or locked from the inside with a sturdy sliding bolt lock or other similar device or equipped with bars or grills.

Overhead roll doors not controlled or locked by electric power should be protected by slide bolts on the bottom bar. Chain link doors should be provided with an iron keeper and pin for securing the hand chain. The shaft on a crank operated door should be secured. A solid overhead, swinging, sliding, or accordion type garage door should be secured with a cylinder lock or padlock. Also, a metal slide bar, bolt, or crossbar should be provided on the inside. Metal accordion grate or grill-type doors should have a secured metal guide track at the top and bottom and be secured with a cylinder lock or padlock.

Windows:

Windows are another vulnerable point for gaining illegal access to a building. Windows should be secured on the inside using a lock, locking bolt, slide bar, or crossbar with a padlock. The window frame must be securely fastened to the building so that it cannot be pried loose. As with glass panels in a door, window glass can be broken or cut so the intruder can reach inside and release the lock.

Bars and steel grills can be used to protect a window. They should be at least one-half inch in diameter, round, and spaced apart six inches on center. If a grill is used, the material should be number nine-gauge two-inch square mesh. Outside hinges on a window should have non-removable pins. The hinge pins should be welded, flanged, or otherwise secured so they cannot be removed. Bars and grills must be securely fastened to the window frame so they cannot be pried loose.

Manholes, Grates, and Storm Drains.:

Many facilities have manholes and tunnels providing service entrance into buildings. Other manholes may provide entrance to tunnels containing pipes for heat, gas, water, and telephone. If a tunnel penetrates the interior of a building, the manhole cover should be secured. A chain or padlock can be used to secure a manhole. Steel grates and doors flush with the ground level may provide convenient access. These openings may be designed into the facility as they may provide light and ventilation to the basement levels. If the frame is properly secured, the grates or doors can be welded into place or they can be secured with a chain and padlock. Sewers or storm drains that might provide an entrance should be secured.

Mechanical Areas:

Prevent Public Access to Mechanical Areas. Mechanical areas may exist at one or more locations within a building. Some mechanical areas have access from the perimeter, other mechanical areas may only have access from the interior of a facility. These areas provide access to centralized mechanical systems (HVAC, elevator, water, etc.) including filters, air handling units, and exhaust systems. Such equipment is susceptible to tampering and may subsequently be used in a chemical, biological, or radiological attack. Keyed locks, keycards, or similar security measures should strictly control access to mechanical areas. Additional controls for access to keys, keycards, and key codes should be strictly maintained.

Restrict Access to Building Operation Systems by Outside Maintenance Personnel. To deter tampering by outside maintenance personnel, a building staff member should escort these individuals throughout their service visit and should visually inspect their work before final acceptance of the service. Alternatively, building owners and managers can ensure the reliability of pre-screened service personnel from a trusted contractor.

Human Barriers:

The word Human Barriers connotes to form an barrier as a first line of defense in the security industry, a line of people standing next to each other with their arms linked, in order to defend or protest against any kind of Anti-social activity.

Animal Barriers:

Animal barrier security measures usually means with the recent threat levels across nation the industries and the different institutions have started to adopt the newer trend in the security measures to the organization, Animal barrier popularly know as Dog barrier , it means sniffer dogs used to detect explosives and other IED's (Improvised Explosives Devices) in the vehicles, after the 26/11 attack in one of the renowned start hotel in Mumbai , now almost all the hotels in that category have come up with the sniffer dog facility. This also acts as a deterrence measures to the public and the anti-social elements. Hence this forms as a one of the barrier in the security measures

UNIT-II: DUTIES OF SECURITY STAFF

In a world that is becoming so desperate and violent day by day, it becomes increasingly important to ensure your personal security as well as that of your office and the premises. Almost all the security staffs are rigorously trained these days before they are deployed at a site to work to prevent any kind of criminal activity at any point of time. Both armed and unarmed security personnel possess the skills to ward off the intention of a criminal or an anti-social element in the society, however they have other duty as well apart from the handling the criminals.

A detailed description of the persons who are eligible or in eligible to be a Security guard or supervisor is given in the sec 10 of the PSARA (Private Security Agencies Regulations Act) 2005. A security agency shall not employ or engage any person as a security guard or supervisor rank personnel unless he is eligible to be so employed or engaged.

In this unit, the duties of the security personnel in various levels of hierarchy is illustrated.

Some of the key functions of Security:

- Safeguarding the estate and any kind of property and the people working therein.
- Screening of the visitors entering into the premise.
- It is the first interfacing contact on behalf of the organization at the entrance level.
- Right manners and polite behavior of security staff need not recede the firmness in dealing with the visitors as a known or unknown person.
- Collection of preservation of personal belongings of the visitors in cloak room
- Filtering of walk in visitors without prior information
- Generating visitors pass and identity badge for the purposeful visitors and directing/escorting to the designated areas.
- Precaution in respective of certain safety wears like compulsory helmets wearing for the rider and the pillion rider.
- Physical inspection of the outgoing vehicles in and out to trace out any concealment.
- Patrolling through the campus at the designated intervals.

- Frisking of the person and searching the belongings of the persons while relieving from duties.
- Observing the vigilance duties by checking the locking conditions of the chamber, cabins etc.
- Maintaining the movements of register of the staff, going out and coming in with the permission for personal or official purpose.

Duties of a Security Staff:

- To provide private security to property or a personal or both together.
- To render necessary assistance to the police in the process of any investigations pertaining to the activities of the agency in which he is employed.
- To bring any unlawful incident to the notice of his superior noticed by him during his duty.
- Not to divulge of any kind of information acquired by him during his employment with respect to the work which he has been assigned to by his superior.
- The security guard deployed at the perimeter of the gates of any organization has to do the checks on the vehicle entering the premises at all times, the check of the ID card of the working personnel in the facility has to be carried out by the guards at all times.
- The security must render assistance to the parking areas where in the vehicles are parked.
- The security guard must carry out the frisking of all the contract staffs in the premises to ensure that no company assets are being carried out without any proper authorization.
- The security guard must carry out patrol of the premises and report any untoward incident or any kind of suspicious activity to his superior for the necessary action.
- The security guard must be well trained and aware of the Firefighting techniques through the Fire hydrant line and Fire extinguishers.
- The security guard is expected to maintain basic registers that are maintained at any organization in a flawless manner at all times and the same has to be checked by the supervisors from time to time.

Duties of a Security Supervisor:

Security supervisor is the most important post of security in any industry. He is responsible for total security of a unit where he is doing his duty. Supervisor should have a set of skilled knowledge and understanding and ability to supervise the unit. The following are the scope of security supervisor in any unit.

- A. Guarding Operations** - Checking of guards and giving duties to them and maintains the weekly / fortnightly duty roster.
- B. Security Document** – Should know about muster roll, shift report, duty roster incident and complaint report forms, personnel and vehicle and material movement control documents and key registers.
- C. Site Instructions** - Site layout – perimeter details of entry, exit and emergency exits; work shifts, guard posts deployment of security and surveillance equipment's patrolling and number of personnel needed for each security shift at the facility.
- D. Assessment and operational effectiveness** – Thorough pre-shift briefing and checking surprise checks, patrolling, mock drills and rehearsals.
- E. Leadership and Supervision** – Welfare training and motivation, leading by personal example, impartiality honest reporting and punctuality.

Performance Criteria of shift supervisor.

- He should start the shift as per the given instructions by his superiors.
- Receive and implement instructions from unit superiors.
- Receive and understand shift report from outgoing supervisor.
- Take attendance and record / report shortage.
- Proper duty roster of shift and give duties to guard as assigned work.
- Deploy guard with the required instrument in required site location.
- Make procedure to collect intelligence and information
- Maintain key control, personnel control for the unit.
- Ensure co-ordination with EHS (environment health and safety) and control room personnel's.
- Train security guards on different job profile.
- Maintain all document as per security responsibility.
- Keep communication with guards, unit incharge & security team.

- Keep the turnout, morale of the unit high.

Duties of Security Officer:

A security officer plays many different roles, but his primary task is to prevent crime. The presence of security officer on the premises often serves as a deterrent to potential lawbreakers. Security guards work in public and private buildings, as well as retail and wholesale establishments. Working as a security officer comes with a significant level of responsibility so prospective candidates must be able to demonstrate

- A polite but firm approachable manner at all times
- A reasonable of physical fitness and strength
- A trustworthy character
- A Flexible and responsible approach to job.
- The ability to be patient regardless of situation.
- Good verbal and written communication skills
- The ability to solve problem as they raise
- A basic knowledge of Information Technology
- The ability to follow instructions.
- A confident approach and ability to deal with the difficult and confronting people.
- The ability to work independently and as part of the team.
- A good knowledge of customer care.
- A non- judgmental approach.
- The ability to relate well to wide range of people
- The ability to respond positively to stressful situations.
- A clean criminal record.

Security Officers are responsible for maintaining the security of people, buildings and their contents, preventing break-ins and theft through guarding and surveillance. They are expected to deal with a wide range of situations as they occur. The roles of security officers will vary depending on the industry they work for. Security officers work in a range of environments, ensuring that businesses, properties and valuables are protected from harm.

As security officers perform their job, they often patrol both the interior and exterior of the premises where they work. They monitor windows, doors and gates to make sure they're locked properly. If an alarm sounds or there's a disturbance, the security officer is the first on the scene, and is often the one making the call to emergency police, fire or ambulance services. Security officers might have the responsibility of taking phone calls that come into the business after hours. Some have the task of monitoring the heating and cooling systems of the buildings they guard. Security officers prepare daily activity logs and reports of any damage to equipment to present to their supervisor.

The role of a security officer varies from day to day; they must be quick-thinking and deal with situations as they arise. Responsibilities typically include

- Patrolling one or a more number of premises
- Monitor activities inside and outside the premises through observation and Closed-Circuit television
- Signing in visitors to the building and maintains the visitor management system and adherence to the protocol laid by the organization.
- Sorting post and checking suspicious packages.
- Performing checks on building traffics.
- Recording any suspicious activity and taking any necessary action.
- Guarding valuables or cash
- Communicating relevant information to other security officers via Walkie – Talkie or other communication devices.
- Handling sniffer dogs
- Writing reports for the police or court in case of any incident recorded
- Conducting general reception duties.
- Creating and distributing ID cards and Access cards.

Duties of Chief Security Officer:

As the word CSO connotes to, "chief security officer" means what it sounds like. Broadly, a CSO is the highest-level executive directly responsible for an organization's entire end to end

security function. Increasingly, CSOs are not only responsible for their organizations' physical security needs but also their digital or electronic security requirements, including computer networks. Originally a title used to designate the person most responsible for information technology security, the new CSO executive looks at all threats and institutes appropriate security programs.

A CSO is the executive whose ultimate role is to ensure that an organization's security function adds value (Chief Security Officer) and gives it a competitive advantage. A major part of a CSO's role within an organization is to help forge strong and secure connections between departments. For example, when corporate departments worry less about security vulnerabilities all around them, they may operate more smoothly with each other. A CSO who can reduce friction between departments thus adds value to an organization

The responsibilities of the CSO is usually executives, and many corporations want them to have advanced degrees in business or come to the position with significant security experience. For instance, many CSOs come from law enforcement backgrounds and have computer training if they're responsible for IT security in their organizations.

UNIT-III: SECURITY SYSTEMS

In the recent past, the crime rate in India is rising every year. Based on recent NCRB data (National Crime Records Bureau), crime related to property constitutes a massive 22% of total crime in India. Conventional security measures such as locks, watchmen and guard dogs are not enough to safeguard your home. The recent trend in Crimes and its modus operandi have made the security system both Physical and Electronic systems more robust in nature and has become mandate almost in all the organization across different sectors.

In this chapter, one shall have an overview of what is the Interrogation and Investigation and taking of the statements / Confessions reports from the alleged person, Public relations and its importance and the participation in Industrial security, Use of sniffer dog in the modern day security context.

Interrogation:

The word “Interrogation connotes to Questioning of a person who is involved in an act which is not acceptable and questionable”. The formal questioning of suspects or person in order to obtain incriminating information and or a confession. Person is expected to be reluctant & uncooperative to divulge information concerning offense or a criminal act. Generally, interrogations are designed to record what witnesses to an offence observed, not what they thought about it. Nevertheless, the witnesses ' opinions and intuition can provide enforcement officers with leads that can be tested through asking further questions about why the witnesses think what they do.

Purpose of Interrogation:

- Establish innocence of guilt by questioning the suspect
- Gather facts objectively without bias
- Discover leads towards new evidences, motives witnesses or suspect.
- Discover leads for another case
- Establish link which connects and / or verify facts supplied by different people or facts learned in previous questioning of a same person.

- Confession or Admission of the act committed.
- Discover the truth

Interrogation Techniques:

- Assumptive questions, the questions are to be the open ended and leading question to the suspect.
- The interrogator should watch for the timelines- immediate is good and reliable, delayed response is not good and may be the interrogator has to ponder over more on the same.
- The interrogator should have more of observer's skills, he or she has to observe the interviewee's behavior and body language.
- Timing of deceit indicators must coincide with stress questions.

Investigations and taking of Statements:

Investigation, the primary purpose and goal to conduct a Investigation is to have an interaction to elicit the maximum amount of truthful statement made, the interviewer has to obtain the greatest quality and quantity of information from the interaction. The interview must be planned in the three stages Before, During, After the interview.

The investigation is an art which deals with the collection of Facts to accomplish the three main parts To Identify the suspect, to locate the suspect and to prove the evidence of of his guilt or innocence

The following are the characteristic of good investigator:

- The ability to preserve or stick to the task despite of the monotony and the many obstacles which surrounds it.
- He must have certain abilities and an intelligence which would enable him to acquire information easily and readily and to use this information truthfully.
- He must be honest. He must be incorruptible and must possess personal integrity.

- He must have understanding (weakness and strength) of the people and the environment where he/she lives.

The following are the six cardinal rules and golden rules for a good investigator:

- When – Where – Who – What – Why – How – Identify and if possible, retain for questioning the person who first notify the first responder.
- Determine the perpetrator by direct inquiry or observe him, if his identify is immediate apparent.
- Detain all person present at the scene if possible for enquiry
- Summon assistance if needed through an authority or competent person
- Safeguard the area by issuing appropriate orders and/ or by physically isolating it.
- Permit only authorized person to enter the area
- Separate the witness to obtain independent statements.
- Do not touch or move any object
- Assign the duties of search if assistance are present.

Every interrogation or an enquiry must requires a statement of record to be obtained by the interrogator or the person who has investigated to the issue, statement plays a significant role in conducting the investigation where in the facts and figures of the case is recorded. The below are the importance of obtaining the statements based on the interview / interrogation conducted by the competent authority.

- Information discovered to date can be traced and it becomes easier to determine where to take the investigation next.
- Statements are useful for briefing witnesses if they are to appear in court later; their earlier statements can be used as a starting point.
- Witnesses can use statements to remind themselves in court if they were made at a time when the events recorded in it were fresh in their memory
- A statement may still be admissible as evidence even when the witness has forgotten some of what was said, provided that the information is useful and reliable for the court
- If a witness makes mistakes in court, the prosecutor can correct them by offering a previous statement in relation to the facts of the case.

- If a prosecution witness becomes hostile, the prosecutor can (with the judge's leave) cross-examine the witness using previous statement to show inconsistency: (s37(4)(a) of the EA). In this way, the prosecutor may limit damage done to the case by casting doubt on the witness's disposition to tell the truth.
- A statement can be used in court to back up what a witness has said, if the defence challenges the ability to provide an accurate and truthful account due to a previous but recent inconsistent statement or claim.
- A statement might be admitted if the statement-maker is unavailable as a witness, so long as the circumstances provide reasonable assurance that it is reliable.

Liaison with local police and personnel:

The word liaison connotes to “communication or cooperation which facilitates a close working relationship between people or organizations”. In an any successful organization, the liaison role plays a significant area which facilitates horizontal information flows, it promotes understanding and enforces process. The nature of the interactions between business and IT units is an important element of a company's competitive success and is a key determinant of success or failure.

Especially in any organization the Security department head also plays major role in Liaising with the governments namely Police, Fire and other licensing authorities, this is intern will help the organization in a flawless operation and also it will help to achieve the greater heights in all aspects.

Use of Dogs in Industrial Security:

Well trained dogs can be used with great advantage to supplement the efforts of security personnel in protecting the assets. This is particularly so, where the facility is protected under vast areas of patrolling design. Dogs are generally used for guarding, sniffing out explosives and also for personal protection purpose in industrial security. There is no single breed of dog which can perform all these three functions effectively. Dogs are to be trained for specific duties. During training the dog is taught to develop its faculties for a particular function, thus a dog trained for guard duties will be a failure if the same dog is deployed for detecting explosives, even if it has a

excelled sense of smell. The reason is simple that it has not been trained for that purpose. Since most of the security managers in the different sectors are interested in utilizing dogs for guard duties and sniffers we are dealing with this subject in an elaborate manner.

Commonly used breeds are:

Alsatian – This type of dog breed is mainly used for guard duties, but on the other hand they can also be used as a sniffer dogs.

Labrador – this type of dog breed is specifically used for sniffing duties (in the recent past , the Hotel security sectors are using this type of dog).

Doberman – for protection and attacking purpose incase if there is need for the same.

Alsatian:

This breed is also known as German Shepard Dog, most intelligent breed among dogs as they are fearless without being aggressive and have an appearance which is consistent with the popular image of guarding dog. They are sturdily built and possess the strength to work hard in all types of climate. As they have an sense of self preservation they react quickly to dangers alert to every sight and sound and always ready to attack. They are very loyal their master (Handler) their powers of hearing and scent are phenominal but their eyesight is week. They can work if the occasion demands, non-stop for over fourteen hours.

Selection of Dogs plays a vital role, grown up dogs are very difficult to train hence to obtain satisfactory results pups should be brought from the reputed breeders who can furnish kennel club India certification. It is better take along a Veterinarian. The dog and a handler should be sent to a well-established training facility to teach the dog to obey commands to perform guard function, tracking, searching for strangers and attack them as and when need arises.

Labradors:

Labradors are mainly used as sniffer dogs to locate explosives. They are very friendly dogs to children if they are to be deployed effectively on explosives detection duties, they should be kept

away from children and people. They should not be used in facilities where there is overpowering scent of gasoline, chemicals etc..

Doberman:

This particular breed is used as a protection dog, Dobermans are good attackers, they should not be used as guard dogs as they would attack often without provocations they can be used effectively for executive protection. The normal practice is to allow a Doberman to stay loose in the executive suite and attack any potential source of threat.

Economics of the use of Dogs:

Compare to the wages of security personnel, maintenance of dogs is very expensive, it is cheaper to use a pair of security personnel for patrolling than using a team of a dog and a handler. Use of dog is therefore made on considerations of actual need. In large facilities with extensive grounds it is advisable to use a team of dog and a security personnel on patrol duties to locate potential anti-social elements. Dogs are also useful to provide warnings to security personnel of hidden dangers; Human beings cannot do these. Use of dogs therefore is dictated by actual security needs by the respective Security managers in the industry.

UNIT-IV: SURVEILLANCE

The word surveillance defines as the monitoring of behavior activities, or other changing information for influencing, managing, directing, or protecting people. This can include observation from a distance by means of electronic equipment (such as closed-circuit television (CCTV) cameras or interception of electronically transmitted information (such as Internet traffic or phone calls). It can also include simple no- or relatively low-technology methods such as human intelligence agents and postal interception. The word surveillance comes from a French phrase for "watching over" (sur means "from above" and veiller means "to watch") and is in contrast to more recent developments such as so

Covert Surveillance:

Intrusive surveillance is defined as "covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device."

Overt Surveillance:

Overt surveillance is called as an investigation technique that is carried out using devices that are visible and obvious Overt surveillance is visible security like security agents at the mall and security cameras in casinos. With overt surveillance, people know the surveillance equipment is there to make sure no one is stealing or cheating and it creates a deterrence among the public at large.

Foot Surveillance:

Foot Surveillance requires intense concentration as the smallest amount of time when the subject is not in view result in the subject being lost amongst the crowd.

- It may not always be possible to observe the subject directly, in that instance the investigator must observe the general area around the subject such as aisles within a supermarket or clothing store.

- Foot surveillance may require the investigator to travel by train, tram, bus or other forms of transport as such it is imperative that the investigator remain as inconspicuous as possible and refrain from any face to face contact with the subject.
- Foot surveillance requires the investigator to think quick and make decisions as to how long to maintain close surveillance without alerting the subject, proficiency comes from experience in relation to this and other forms of surveillance.
- Foot surveillance should be done from some distance and the investigator should be attired in non-descript clothing, no bright multi coloured clothing. The investigator should attempt to dress and appear mundane.

Automobile Surveillance:

This kind of surveillance is predominantly used by the modern-day security operations and most popularly used in the police department, the effective automobile surveillance acts as a preventive measure in order to prevent crime and antisocial elements, this shall avoid all kinds of risks and threats and any kind of hazard which shall avoid vulnerable situations arising from various crimes, incidents, accidents, emergencies, crowd, aggressive behavior, natural or manmade causes.

Team Surveillance:

A team of skilled and trained people who are into the task of observation can connote to team surveillance, usually buddy system is followed in the case of team surveillance where in two or more is connected and carry out the surveillance method in the potential areas

UNIT-IV: TYPES OF INVESTIGATIONS

The role of security in investigations:

The role of security staffs during investigation of incidents is collecting information and evidences to determine the facts, the information collected must not, contain the security staffs opinion. Any opinion expressed by person questioned must be identified clearly in their report as their opinions. The security officer must collect all available information about the incident, even information that may appear irrelevant at the time.

Investigations Techniques to be followed by the security:

Conduct the investigation at the scene if possible, in some cases because of the nature of the incident, it will be necessary to conduct interview in private. Prior to any statement taking or in dept. inquiry, all the person being interviewed (i.e. Victim, witness or suspect) to tell the entire story without any interruption. The most essential element of any investigation is report writing. An extremely thorough investigation of an accident or incident can have rendered worthless by submitting an inadequate report. The report is both an instrument for transmitting to management immediate information about what happened and is an instrument of factual record that may be submitted to the authorities, insurance company, or attorneys. A good investigation report must consist of the following

1. Who is involved?
2. What happened?
3. Where did it took place?
4. When did it happen and duration?
5. How was it done?
6. Why was it done?
7. Activities or person within the vicinity of scene?
8. Clothing shape or any other description.

The following are the different kind of investigations that can be carried out in the security industry.

Pre-Marital Investigations:

Getting married to someone is a lifelong commitment, and arguably among the most important decisions of one's life. Hence, it is extremely important to perform some basic checks on your partner before committing to a marriage. It is not uncommon in India to lie or manipulate a few facts in order to get a better life partner. Getting into an unhappy marriage not only shatters the dreams one has, but also leaves behind a long, lonely and painful life to live. In order to avoid such a situation and to enable you or your loved ones to take an informed, correct and unbiased decision, the following aspects are to be covered in the Pre-Marital investigations.

- Character Verification of the Spouse (Male / Female)
- Behavioral habits such as (Drinking, Smoking, Spending extravagant)
- Family Background
- Financial Status
- Social Status
- Early marriage
- Employment details like Designation, Tenure, Remuneration and Future prospects.

Post-Marital Investigations:

Marriage is all about trust and faith between two individuals or two families. That's why, we prefer to marry someone we know, or seek union with a family we're sure about. We know risks are great in cases where marriages are made between couples or families that don't know each other in a better manner, however in the recent past due to the societal change and change in the behaviors and life style of the individuals the post marital life becomes an turmoil for many.

Land dispute Investigations:

Disputes involving property and land can often cause distress and frustration. Whether it involves a neighbor, co-owners or a local authority, you may require legal assistance to reach an acceptable solution. Land Law can be complex, which is why seeking a proper professional security investigations and proper legal aid expertise will provide you with peace of mind that the issues are carefully considered with an effective application of law. Property and land

disputes can include damage to your land, boundary disputes, trespassing, ownership issues, rights of way and access to land.

How to handle law disputes:

- Try to avoid dispute at the first place and always aim at an amicable settlement. Communication is key and minor disagreements can escalate into disputes if they are not handled carefully. Keep your neighbors informed about any work/changes you're planning to make to the boundary of your properties before you start work and make sure you keep communication channels open.
- Listen to neighbor's comments and their side of dispute, be prepared to compromise; people often come to us believing that they are 'in the right'. Two opposing parties, both with strong stand points, can often lead to them taking the decision to litigate as a matter of principle without always considering that the journey they are embarking on is a) lengthy, b) costly and c) pursuing a neighbor through the courts will cause irreparable damage to neighbor relations. Not many neighbors can maintain a cordial relationship after suing each other.
- Review land register plans, Land Registry title plans are drawn to a small scale and are not intended to show the precise location of each boundary; indeed, all Land Registry title plans are headed with a disclaimer to this effect. These plans should be checked on site. Don't rely on the accuracy of the Land Registry's Plans. It's a common misconception that these plans are completely accurate, when in fact, they have been created as a guide and often need the insight of both a solicitor who will consider the Title Deeds for a property, review other documentation such as old photographs and a surveyor who may wish to conduct a site visit before the true line of the property boundary can be established.
- **Consult a chartered surveyor arbitrator**, A chartered surveyor arbitrator will also be able to understand the disputed issues faced by the parties in a land, property or construction dispute. The arbitrator's decision is final and binding, although there are limited rights of appeal to the courts on procedural irregularities and a point of law.
- **Litigations is not the only method of handling land disputes**, remember that there are alternatives to litigation available, namely Alternative Dispute Resolution (ADR). A

responsible solicitor should advocate the benefits of mediation in property or neighbor disputes as early as possible and certainly before the issuing of any proceedings. Mediation is significantly cheaper than litigation and can be organized quickly at a time, location and cost agreeable to the parties. Conducted with the assistance of an experienced property litigation lawyer, who has good relationships with mediators, it's an option that can save costs and angst and put parties on the right track to a securing a relatively peaceful resolution.

- **Get an expert support,** incase if the case is peculiar and really struggling with serious disputes without any delay it is advisable to approach a proper

Solicitor

A Registered Land Agent

Student Investigations:

If a student conduct receives a complaint, a report of an incident, or an allegation against a student or a group of students, usually the institutions has their own enquiry committee to deal with the allegations and thereby a separate disciplinary committee is formed where in the individual will be notified in writing within a stipulated period of time by the institutions (normally within 10 working days after the incident is brought to our attention), that an allegation has been made about you which might be a disciplinary offence. You will be given a summary of the allegation(s) against you and will be invited for an interview with the Investigating Officer (IO), in the recent past such cases are being referred to the reputed detective or security agencies where in an external agency carry out an investigation and submits the report to the institution.

The purpose of the interview is:

- to inform you of the allegations.
- to explain the disciplinary procedures.
- for you to respond to the allegations and explain what may have happened.
- for the IO to ask questions to ascertain the facts of the case.

You may bring a “friend” to the interview. A “friend” is defined in the University regulations as an academic member of staff of the University, or a registered student at the University of Birmingham, or a full-time Officer of the Guild of Students. The role of the “friend” is to act as an observer and give moral support. Your “friend” cannot also be a witness to the alleged breach/incident. You are expected to attend the interview. If you do not engage with the process, the investigation will continue. You may also be subject to the charge of “Contempt of the University’s disciplinary procedures by failure to cooperate with the University’s discipline authorities

The interview At the beginning of the interview the IO will introduce themselves and any other people present. Normally there will be a note taker. At the beginning of the interview, you will:

- be informed of the procedures that will be followed in accordance with University Regulation Section 8 - Student Conduct;
- have an opportunity to ask questions about the procedures.

The IO will then confirm the allegations which have been made against you. You will not be entitled to see or receive copies of any statements or evidence at this stage of the procedure, unless the IO decides to disclose it to you. You will not normally be permitted to record the interview. You will be given the opportunity to respond to the allegations and put forward any explanation you may wish to give. The IO will then ask questions of you to try and ascertain the facts of the case. You may discuss with the IO whether any other people may be able to provide information or evidence and you may suggest potential witnesses that you would like the IO to contact. It is, however, for the IO to decide if it is necessary or appropriate to do so. If you provide witness statements for the IO at the interview, please make sure they include contact details in case the IO needs to clarify details with the witness. At the end of the interview the IO will inform you what the next steps may be, depending upon the nature of the allegations, and whether or not the IO considers that there is sufficient evidence to take disciplinary action. It may be necessary for the IO to collate further information before reaching a conclusion; this may include more than one interview with you. A copy of the notes will normally be provided to you at the end of the interview. Once the report has been submitted by the IO (Investigating officer) to the institution the competent authority may take action that is deemed fit and it may vary from case to case.

Kidnapping and Abduction Investigation:

In criminal law, the word kidnapping connotes to an unlawful assortment and confinement of a person against his or her will. ... It can also be defined as false imprisonment by means of abduction, both of which are separate crimes that when committed simultaneously upon the same person merge as the single crime of kidnapping.

Abduction, is when someone uses deceit or force to take a person or a child away from their home or relatives. The abductors do not reveal their motive for taking away the person or the child. Merriam Webster defines 'abduction' as, "to seize and take away (as a person) by force." In legal definition, the victim knows or has some sort of relation with the abductor. The victim can be a minor or an adult. The most common cases of abduction are seen in divorce cases, where one parent is given the sole custody of a child. The person who abducts is not holding the person for profit or any monetary gain from the victim. The laws for abduction crimes vary from state to state and country to country, depending on the severity of the crime.

Kidnapping, is taking away or forcefully transporting a person against their will and holding them in false imprisonment, a confinement without legal authority. The kidnapping is usually done for a motive or for ransom. 'Kidnapping' is defined as, "to seize and detain or carry away by unlawful force or fraud and often with a demand for ransom."

Kidnapping involves taking a person from their family forcefully without their consent with the motive of holding the person as a hostage and earning a profit from their family. The kidnapping could be for a number of reasons such as getting monetary reward, or getting some sort of benefit from the person.

Missing Person Investigations:

A countless number of people go missing every year in all parts of the world that depends on the information you already have and what you need to find out. The necessary steps will be fewer if you have the person's name and you're just looking for a current address or telephone number. Names may be unknown for someone looking for an adopted child or for birth parents. In these

cases, your search will take more time while you contact everyone you think may have a piece of the puzzle—a relative, former neighbor, clergy, lawyer or caseworker.

The first officer deployed to attend a report of a missing person should carry out the following actions:

- establish the facts and keep accurate records of what was said and by whom
- assess the circumstances of the disappearance to judge the risks to which that person and the community are likely to be exposed.
- notify a supervisor to ensure oversight; this should happen immediately in high-risk cases, and as soon as is practicable in all other cases
- gather sufficient information about the missing person to enable an effective and thorough investigation to be conducted; the depth of that information will vary according to the assessment of risk. Very detailed information and a lifestyle profile will be needed in high-risk cases
- consider taking a full statement from the person reporting the missing person as well as any other key individuals (e.g., the last person to see them)
- conduct initial searches of relevant premises, the extent and nature of the search should be recorded.
- consider seizing electronic devices, computers, and other documentation, (e.g., diaries, financial records and notes) and obtain details of usernames and passwords
- obtain photos of the missing person; these should ideally be current likeness of the missing person and obtained in a digital format
- obtain details of the individual's mobile phone and if they have it with them; if the missing person has a mobile phone arrange for a safe text that must be sent by the charity, Missing People
- obtain details of any vehicles that they may have access to and place markers on relevant vehicles on the PNC without delay
- consider obtaining any physical evidence of identity such as fingerprints or DNA samples in accordance with the procedure laid down.
- confirm if the person has taken their passport, (consider prompt circulation if it is deemed likely the individual may leave the country)

- make all immediate relevant enquiries and take immediate actions in order to locate the missing person.
- consider the need for specialist officers or resources, eg, force helicopters, dogs, financial investigation officers.
- upload the missing person report
- circulate details of the missing person on local information systems and to relevant local partners, e.g., hospitals, ambulance service, taxi and bus firms.

It is important for an individual (who has responsibilities/concerns for the missing person) to be identified who can act as the point of contact for the police. The police will agree with the individual/family when they will next be contacted. This person should be provided with a call reference number and given details of how to contact the police with any further information they have about the case or if they would like to receive an update. An assessment must be made of the level of support required for the family, residential worker or foster carer and consideration should be given to appointing a family liaison officer. Information should then be provided regarding additional organisations that may be able to assist or support them.

Traffic Accident Investigations:

One must know how to carry out the investigation when it comes to a traffic accident, and how to obtain witness and victim information, how to determine the cause and fault of an accident and properly fill out the information report and Accident/ Incident form. Investigators should be able to properly clear the scene of an accident calling upon the necessary resources for further assistance in this regard.

Traffic accidents are extremely confusing events. How they occur, who or what caused them, and why they occurred are facts that an Investigation officer must determine. Every peace officer must know the fundamentals of traffic accident investigation and know how to prepare traffic accident reports. Traffic accidents, resulting in personal injury, fatality, and property damage can be of a major impact to the public safety.

The following are the steps to be carried out at the time of Investigating a traffic incident. Prompt arrival at the scene of an accident is essential for the Investigating officer. While in route, the

officer should maintain contact with the Dispatcher. They should also be on the lookout for any suspicious or damaged vehicles fleeing the general area.

- Location
- Time of notification.
- Who notified the officer and how?
- Weather and visibility conditions
- General information as to seriousness of the accident--injuries, hit and run, amount of traffic congestion, etc.
- Whether additional support is proceeding to the scene, such as wrecker, ambulance, or additional Police patrols
- By obtaining such information prior to arrival at the scene, the investigators may more quickly and efficiently respond to the needs of the situation.

Securing Facts at Scene. After completing the initial steps and securing the scene of the accident, the investigator obtains and records facts needed to complete their reports to arrive at logical and objective conclusions. The main thrust of the investigation is to determine whether or not there was a violation of the law; and if so, to prove each element of the offense. Explorers should issue a traffic ticket when appropriate.

Identify and Preserve Fragile Evidence, any fragile evidence that can be damaged easily, altered, destroyed or removed from the scene by any willful or negligent act must be identified and secured. Prior to removal, its position should be noted, sketched, photographed and/or marked in chalk. Examples of such evidence are puddles of gasoline, oil, blood or pieces of broken glass. The position of turn signal levers should be checked; although this is not a positive indicator of whether a turn signal was in use it can be helpful. Alcoholic beverage containers inside a vehicle should also be secured. Evidence should be tagged, marked, and secured in accordance with proper evidence gathering procedures prior to its removal from the scene.

Medical statements may be required to reflect expert opinions as to whether medical reasons contributed to an accident. The investigator must obtain medical information for the following:

Personal injuries--Determine the extent of injuries received by all involved in an accident and any injuries that existed prior to the accident.

Fatal injuries--In case of deaths, obtain estimated time and cause of death.

Tests--Obtain any information concerning the results of alcohol, drugs or medicine used. The accident investigator should recommend to all persons involved in serious accidents that they see a physician immediately.

Pre-employment verification and Post Employment:

An employer's viability frequently depends on the quality and reliability of its employees. As a result, employers often spend significant amounts of money and time in recruiting and interviewing prospective employees to hire individuals who are best suited to perform a job. Employers also screen prospective employees to limit potential legal liability. Although there are a variety of ways in which the law can hold an employer liable for an employee's actions, the doctrine of vicarious liability and the tort of negligent hiring are the most significant. Having an effective pre-employment process for hiring new agency staff can be the most critical step in hiring and retaining quality employees and minimizing potential liability exposure and workplace wrongdoings, including.

A prospective employer also checks on the below criteria before selecting the right candidate for the employment civil rights claims – race, religion, age, disability, disparate impact, violation of Equal Opportunity laws, etc.) Negligent Hiring, - General liability claims - Employee injuries - Vehicle accidents - Violence in the workplace - Workplace theft

Post-Employment Verification:

The post-employment checks and investigations plays a pivotal role in the modern-day world, the checks that are made on the employees who are already serving the organization. The checks and the preliminary investigations are made in a highly professional and discreet manner If any employee is cheating or doing frauds with the management of the company then they will be unveiled through this investigation. Employees that are designated in higher profile have much

potential to access the confidential details of the company. The confidential details of a company should be kept secret always and if it is misused, then the reputation of the company will be harmed adversely.

So, to prevent this type of problem post-employment verification is conducted. With this type of verification, the owners can easily evaluate the loyalty of the employees towards the organization.

- Your public records – Companies can easily access your court records and criminal history from any law enforcement agency.
 - Your work history – Companies will dig up your past employers, dates you worked with them, your role in each company, your pay, performance history, your conduct in the company and so on. And don't forget the drug test results!
 - Education records – Companies will reach out to your university to match your credentials. This is a sure thing because forging degrees, fake certificates and bogus grades are the most common types of corporate frauds.
 - Address verification – Who lies about their address, right? The ones who are trying to hide their past, that's who.
 - Aadhaar verification – Did you forget they have your biometrics? And practically every other information about your residence and bank accounts stored in your Aadhar?
 - National Academics Depository (NAD) – Government launched NAD to digitally store your education records. NAD can also issue reliable certificates to verified users since they plan to have every education board and institution in India onboard the platform.
 - National Skills Registry (NSR) – NSR is the largest database of working professionals that helps companies fact-check employees' information (if they are registered) and currently they have about 200 companies with 21,87,635 registered professionals and 14,77,518 biometrics submitted to the database.
-

RECOMMENDED READINGS:

1. Angela Woodhull (2002) Private Investigation: Strategies and Techniques, Texas: Thomas Investigative Publications.
2. Bill Copeland (2001) Private Investigation: How to be successful, Absolutely zero loss Inc.
3. Chaturvedi, T.N., (1991). Indian Banking: Crime and Security in Indian Banks, New Delhi: Aashish Publishing House.
4. Chitkara M.G. (1997) Corruption 'N' Cure, APH Publishing Corporation, New Delhi
5. Douglas Cruise (2002) The Business of Private Investigations, Texas: Thomas Investigative Publications.
6. Haldar Dipak (1986) Industrial Security in India, Ashish Publishing House, New Delhi.
7. Louis and Lawrence (1999) Investigations: 150 Things, Butter worth – Heinemann.
8. Michael Corun (2003) Training Manual on Private Investigation, Texas: Thomas Investigative Publications.
9. Mitra Chandan (1998). The Corrupt Society, Viking, Delhi.
10. Rajaram (1993) Bank Security: A Branch Manager's Handbook, Himalaya Publishing House, Bombay.
11. Ranjit Sen Gupta (1994) Management of Internal Security, Lancer Publishers, New Delhi.
12. Richard S. Post and Arthur A. Kingsbury (1973) Security Administration: An Introduction, Charles C. Thomas, Springfield Illinois.
13. Rojer J. Willand (1997) PI: Self-study guide on becoming a private detective, Paladin press.
14. Rosy J. Methahon (2000) Practical Handbook for private Investigations, CRC Press.
15. W. John George Moses (2004) Materials for Diploma in Private Investigation, Institute of Intelligence and Investigation, Eagle's Eye Detective Agency, Chennai

Related website

1. www.slideshare.com
2. Security knowledge and skill development Council (National Skill Development Corporation)

S. Naresh Kumar Asst Prof & Head,
Criminology, Karunya University,
Periyanaickenpalayam, Coimbatore - 641019